

(19) 世界知的所有權機關
國際事務局



(43) 國際公開日
2004 年 2 月 5 日 (05.02.2004)

PCT

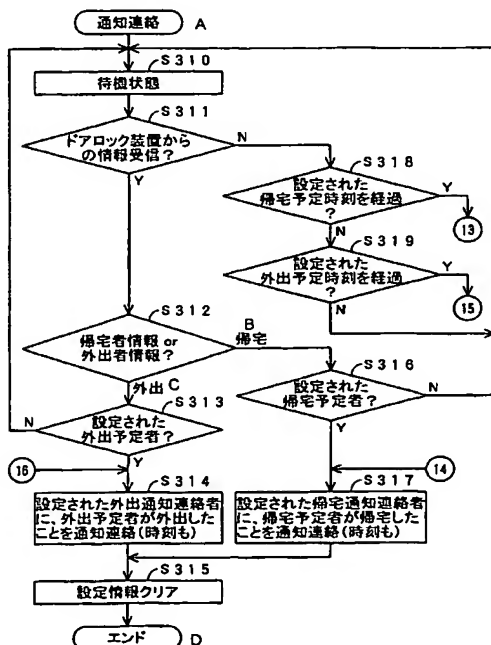
(10) 国際公開番号
WO 2004/011746 A1

- | | | | |
|-----------------------------|-----------------------------|----|--|
| (51) 国際特許分類 ⁷⁾ : | E05B 49/00, G08B 25/04 | | (71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP). |
| (21) 国際出願番号: | PCT/JP2003/009755 | | |
| (22) 国際出願日: | 2003 年7 月31 日 (31.07.2003) | | (72) 発明者; および |
| (25) 国際出願の言語: | 日本語 | | (75) 発明者/出願人 (米国についてのみ): 油井 康二 (YUI, Yasuji) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 松村 広幸 (MATSUMURA, Hiroyuki) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). 八重樫 章 (YAEHASHI, Akira) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP). |
| (26) 国際公開の言語: | 日本語 | | |
| (30) 優先権データ: | | | |
| 特願2002-223700 | 2002 年7 月31 日 (31.07.2002) | JP | |
| 特願2002-278436 | 2002 年9 月25 日 (25.09.2002) | JP | |
| 特願 2002-298309 | | | |
| | 2002 年10 月11 日 (11.10.2002) | JP | |
| 特願 2002-302996 | | | |
| | 2002 年10 月17 日 (17.10.2002) | JP | (74) 代理人: 中村 友之 (NAKAMURA, Tomoyuki); 〒105-0001 東京都港区虎ノ門1丁目2番3号 虎ノ門第一ビル9階 三好内外国特許事務所内 Tokyo (JP). |

[統葉有]

(54) Title: COMMUNICATION DEVICE

(54) 発明の名称: 通信装置



A...NOTIFY
S310...STANDBY STATE
S311...INFORMATION RECEIVED FROM DOOR LOCK DEVICE?
S318...SCHEDULED ARRIVAL TIME PASSED?
S319...SCHEDULED DEPARTURE TIME PASSED?
S312...INFORMATION OF ARRIVING PERSON OR DEPARTING PERSON?
B...ARRIVAL
C...DEPARTURE
S316...PERSON SCHEDULED TO ARRIVE
S313...PERSON SCHEDULED TO DEPART
S314...NOTIFY PERSON, WHO IS DESIGNATED TO BE NOTIFIED OF
DEPARTURE, THAT PERSON SCHEDULED TO DEPART HAS DEPARTED (AND
TIME AS WELL)
S317...NOTIFY PERSON, WHO IS DESIGNATED TO BE NOTIFIED OF ARRIVAL,
THAT PERSON SCHEDULED TO ARRIVE HAS ARRIVED (AND TIME AS WELL)
S315...CLEAR ESTABLISHED INFORMATION
D...END

(S7) Abstract: A communication device that can urge a person who has gone out, for example, a child to come home when it is a scheduled time to do so, and that can notify, for example, his or her parent of a time when he or she will come home. There is provided door lock control means that uses first communication means to communicate with an electronic key device storing at least electronic key information, and that compares received electronic key information with the electronic key information stored in a memory part to control, based on a result of the comparison, the lock mechanism of the door. There is also provided user-identifying means that identifies, based

〔統葉有〕



(81) 指定国 (国内): CN, KR, US.

添付公開書類:

— 国際調査報告書

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

on information received from the electronic key device via the first communication means, the user of the electronic key device. Transmission control means causes, based on a result of identification made by the user identifying means, information concerning arrival and departure of the user of the electronic key device to be transmitted to a predetermined destination via second communication means.

(57) 要約: 外出していたもの、例えば子供に帰宅予定時刻になったときに帰宅を促すことができると共に、当該子供の帰宅時刻を、例えば親にも通知連絡することができるようにした通信装置を提供する。第1の通信手段により、少なくとも電子鍵情報を記憶する電子鍵装置と通信を行ない、受信した電子鍵情報と、記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいてドアのロック機構を制御するドアロック制御手段を備える。また、第1の通信手段を通じて電子鍵装置から受信した情報に基づいて電子鍵装置の使用者を認識する使用者認識手段を設ける。送信制御手段は、使用者認識手段での認識結果に基づいて、電子鍵装置の使用者の入退出に関する情報を、予め定められている通知先に第2の通信手段を介して送信するように制御する。

明 細 書

通信装置

5

技術分野

この発明は、電子鍵情報を用いてドアの施錠、開錠を制御するようにするドアロック制御システムに用いて好適な通信装置に関する。

10 背景技術

最近、従来の物理的な鍵を鍵シリンダーに差し込んで施錠、開錠を行なうドアロック制御システムを玄関ドアなどに採用している住戸等においては、鍵シリンダー機構に精通しているものが、鍵を用いずに開錠することによる盗難等の事件が発生している。

15 そこで、このような鍵シリンダー機構を用いない電子鍵装置によるドアロック制御システムが注目されている。例えば、この電子鍵装置によるドアロックシステムの一例として、親機は、予め登録されている電子鍵情報としてのIDコードと、電子鍵情報としての子機から受信したIDコードを比較照合して、その比較結果に基づいてドアロックをコントロールするものが知られている（例えば特許文献1（特開平9-4293号公報参照））。

20

例えば、外出した子供に、所定の時刻までに帰宅するように約束させた場合であっても、子供はその時刻を失念してしまうことはよくある。この場合に、家に親がいれば、子供が約束の時刻に帰宅していない場合には、親が子供の携帯電話端末などに電話をかけることにより帰宅を促すことができる。

25

しかし、親が共に仕事等で外出していて留守にしている場合、子供が所定の時刻に帰宅したかどうかを確認することができない。そのため、子供に帰宅を促すことができない。

子供に、帰宅時に親に電話させるなどの方法により帰宅を知らせるよう
5 うにすることも考えられる。しかしながら、電話により帰宅の連絡を受けたとしても、本当に帰宅したかどうかを確認することはできない。

この発明は、上述の点にかんがみ、外出していたもの、例えば子供に帰宅予定時刻になったときに帰宅を促すことができると共に、当該子供の帰宅時刻を、例えば親にも通知連絡することができるようにした通信
10 装置を提供することを目的とする。

発明の開示

上記課題を解決するために、請求項 1 の発明による通信装置は、少なくとも電子鍵情報を記憶する電子鍵装置と通信を行なう第 1 の通信手段
15 と、通信ネットワークを通じて情報送信を行なうための第 2 の通信手段と、電子鍵情報を記憶する記憶部と、前記第 1 の通信手段を通じて前記電子鍵装置から受信する電子鍵情報と、前記記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいてドアのロック機構を制御するドアロック制御手段と、前記第 1 の通信手段を通じて前記電子鍵装
20 置から受信した情報に基づいて当該電子鍵装置の使用者を認識する使用者認識手段と、前記使用者認識手段での認識結果に基づいて、前記電子鍵装置の使用者の入退出に関する情報を、予め定められている通知先に前記第 2 の通信手段を介して送信するように制御する送信制御手段と、を備えることを特徴とする。

25 また、請求項 2 の発明は、請求項 1 に記載の通信装置において、前記通知先に入退出に関する情報を送信すべき前記電子鍵装置の使用者の設

定を受け付けて記憶する設定記憶手段を備え、前記送信制御手段は、前記設定された前記電子鍵装置の使用者の入退出に関する情報を、前記第2の通信手段を介して前記通知先に送信することを特徴とする。

この発明による通信装置においては、使用者認識手段は、電子鍵装置と通信を行なってドアの開閉をした者が誰であることを認識する。送信制御手段は、予め設定された通知先に電子鍵装置の使用者の入退出に関する情報を送信する。

したがって、例えば通知先を外出している親としておくことにより、例えば子供の帰宅や外出に関する情報を親に通知することができる。

また、請求項3の発明は、請求項2に記載の通信装置において、前記設定記憶手段では、前記電子鍵装置の使用者と共に、当該使用者に対応して時刻情報の設定入力を受け付けて記憶し、前記送信制御手段は、前記設定入力された時刻情報に対応する時刻を経過しても、前記使用者認識手段で前記設定された前記電子鍵装置の使用者を認識しなかったときに、当該電子鍵装置の使用者の入退出がなされていないことに関する情報を、前記通知先に前記第2の通信手段を介して送信するように制御することを特徴とする。

請求項3の発明においては、例えば帰宅予定時刻を設定しておくと共に、通報先を帰宅予定者と設定することにより、設定された時刻を経過しても帰宅予定者が帰宅していないときには、当該帰宅予定者にその旨を通知することができる。また、通報先として帰宅予定者以外の者、例えば親に設定しておけば、親に帰宅予定者が帰宅していないことを通知することができる。

図面の簡単な説明

図1は、この発明のドアロック制御システムの実施の形態で用いる識

別情報の概要を説明するための図である。

図 2 は、この発明の実施形態で用いる識別情報の一例を示す図である。

図 3 は、この発明によるドアロック制御システムの実施形態が適用された通信システムの概要を説明するための図である。

5 図 4 A および図 4 B は、この発明による電子鍵装置の一実施形態を示す図である。

図 5 は、この発明による電子鍵装置の一実施形態の構成例を示すブロック図である。

10 図 6 は、この発明による電子鍵装置の一実施形態の動作を説明するためのフローチャートである。

図 7 A および図 7 B は、この発明による電子鍵装置の他の実施形態を示す図である。

図 8 は、この発明による電子鍵装置の他の実施形態の構成例を示すブロック図である。

15 図 9 は、この発明による電子鍵装置の他の実施形態の動作を説明するためのフローチャートである。

図 10 A および図 10 B は、実施形態のドアロック制御システムを構成するドアロック装置の一例の要部を説明するための図である。

20 図 11 は、図 10 A および図 10 B のドアロック装置のドアロック制御装置の構成例を示すブロック図である。

図 12 は、セキュリティシステムに用いる監視制御装置の例を示す図である。

図 13 は、図 12 の監視制御装置の構成例を示すブロック図である。

図 14 は、個人プロフィール情報の一例を示す図である。

25 図 15 は、セキュリティモードの内容を説明するための図である。

図 16 は、セキュリティモードの内容を説明するための図である。

図 1 7 は、管理サーバ装置の構成例を示すブロック図である。

図 1 8 は、図 1 2 の監視制御装置の伝言記録および再生機能を説明するためのフローチャートである。

5 図 1 9 は、ドアロック制御モードの設定動作を説明するためのフローチャートである。

図 2 0 は、ドアロック制御モードの設定動作を説明するためのフローチャートである。

10 図 2 1 は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図 2 2 は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

15 図 2 3 は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図 2 4 は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

20 図 2 5 は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

25 図 2 6 は、ドアロック制御モードの一つの例であるオートロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図 2 7 は、ドアロック制御モードの一つの例である逐次ロックモード

でのドアロック制御動作を説明するためのフローチャートの一部である。

図 28 は、ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

5 図 29 は、ドアロック制御モードの一つの例である逐次ロックモードでのドアロック制御動作を説明するためのフローチャートの一部である。

図 30 は、監視制御装置のリモートコマンドからの信号の受信処理動作を説明するためのフローチャートである。

図 31 は、監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

10 図 32 は、監視制御装置におけるセキュリティモードオン時の動作を説明するためのフローチャートの一部である。

図 33 は、監視制御装置におけるドアロック装置との連携動作を説明するための図である。

15 図 34 は、この発明における実施形態において、本鍵情報の登録を説明するためのフローチャートを示す図である。

図 35 は、この発明における実施形態において、本鍵情報の登録を説明するためのシステム構成を示す図である。

20 図 36 は、この発明における実施形態において、帰宅予定あるいは外出予定の設定処理を説明するためのフローチャートの一部を示す図である。

図 37 は、この発明における実施形態において、帰宅予定あるいは外出予定の設定処理を説明するためのフローチャートの一部を示す図である。

25 図 38 は、この発明における実施形態において、帰宅予定者あるいは外出予定者に関する通知連絡処理を説明するためのフローチャートの一部を示す図である。

図 3 9 は、この発明における実施形態において、帰宅予定者あるいは外出予定者に関する通知連絡処理を説明するためのフローチャートの一部を示す図である。

図 4 0 は、この発明における実施形態において、帰宅予定者あるいは
5 外出予定者に関する通知連絡処理を説明するためのフローチャートの一部を示す図である。

発明を実施するための最良の形態

以下、この発明による通信装置の実施形態を含む通信システムを、図
10 を参照しながら説明する。

以下に説明する通信システムでは、家の玄関ドアに、電子鍵装置と電子鍵情報の通信を行なって施錠、開錠を制御するようにするドアロック制御システムを設ける。また、この例では、家の中には、窓や玄関ドアからの賊の侵入、火災の発生、ガス漏れを検知して、それぞれの異常事
15 態に対応する措置を取るセキュリティ監視システムを設け、このセキュリティ監視システムとドアロック制御システムとを、通信可能に接続して連動させて動作させるようにしている。

そして、さらに、この例では、セキュリティ監視システムは、通信ネットワークを通じて管理サーバ装置に接続して、全体として、通信シス
20 テムを構成している。

そして、この例においては、ドアロック制御システムを構成する後述のドアロック装置と、セキュリティ監視システムを構成する後述の監視制御装置とにより、この実施形態の通信装置を構成している。

また、この実施形態においては、電子鍵装置は、生体情報取得部と、
25 制御用 IC (Integrated Circuit) と、通信手段とを備えるもので、種々の形態のものが使用可能である。この例では、こ

の電子鍵装置の具体例としては、ＩＣカードの他、携帯電話端末、ＰＤＡ（Personal Digital Assistants）端末などを用いることもできる。

電子鍵装置に搭載される制御用ＩＣは電子鍵情報用メモリを備え、その電子鍵情報用メモリには、電子鍵情報が格納されている。この電子鍵情報としては、この例では、同一のものが存在しないように一元管理された識別情報が記憶される。この例では、この識別情報としては、ＩＣチップ製造番号が用いられる。

例えば、図１に示すように、１社あるいは複数社のＩＣチップの製造会社１００１において、製造した制御用ＩＣチップ１００２に対して、一元管理された重複のないＩＣチップ製造番号を付与するようにする。ＩＣチップの製造会社１００１が複数社の場合には、例えば、それぞれのＩＣチップ製造会社１００１に、予め、制御用ＩＣチップ１００２に付与する製造番号を割り当てておくようにすることにより、一元管理される。したがって、製造された制御用ＩＣチップ１００２のメモリには、互いに異なるＩＣチップ製造番号が識別情報として記憶される。

この制御用ＩＣチップ１００２は、ＩＣカード製造工場（あるいは製造会社）１００３、携帯電話端末製造工場（あるいは製造会社）１００４、ＰＤＡ端末製造工場（あるいは製造会社）１００５などに供給されて、それらの制御用ＩＣチップと通信手段とが搭載されたＩＣカード、携帯電話端末、ＰＤＡ端末などが製造される。

図２は、この実施形態で用いられるＩＣチップ製造番号の一例を説明するための図である。

この例のＩＣチップ製造番号は、３桁のメーカー番号と、３桁のカテゴリコードと、４桁のシリアル番号とからなる、合計１０桁の番号（記号を含む）で構成される。

なお、識別情報は、I Cチップ製造番号の限定されるものではなく、同一のものが存在しないように一元管理された情報であれば、どのようなものも使用可能である。また、識別情報は、I Cチップ製造番号と共に、別個にI Cのメモリに記憶するようにしてもよい。

- 5 電子鍵装置の通信手段としては、この例では、電磁誘導や電波を用いた非接触による通信手段が用いられる。この実施形態においては、この通信手段は、例えば数ミリメートル～数十センチメートルの範囲で通信ができるものであればよく、小パワーのもので十分である。

- 次に、この実施形態におけるドアロック制御システムにおいては、玄関
10 ドアには、電子鍵装置によりドアの施錠、開錠を行なえるようにするためのドアロック装置が取り付けられる。この例では、電子鍵装置とドアロック装置との間では、電子鍵情報の通信を行ない、ドアロック装置は、その通信に基づいてドアの施錠、開錠を制御するようにする。

- 以下に説明する例では、電子鍵装置とドアロック装置との間の通信は、
15 電磁誘導を用いた非接触による通信とされており、後述するように、ドアロック装置の一部を構成する電子鍵装置のリード／ライト部を介して、通信が行われる。

- この実施形態では、ドアの施錠、開錠を制御するための電子鍵情報としては、前述したI Cチップ製造番号からなる識別情報が用いられる。
20 この実施形態では、当該家における電子鍵情報として、前述のようにして一元管理された識別情報が内蔵メモリに書き込まれた電子鍵装置の前記識別情報を電子鍵情報として管理サーバ装置に登録することにより、家族構成員のそれぞれが、自分用の電子鍵装置を所有して使用するようになる。

- 25 この実施の形態では、管理サーバ装置は、登録された家族構成員のそれぞれについての電子鍵情報をドアロック装置の電子鍵情報の記憶部に

転送して、電子鍵情報をドアロック装置に登録させるようにする。ドアロック装置は、登録された電子鍵情報と、通信装置としての電子鍵装置から受信した電子鍵情報とを比較し認証して、その結果に応じてドアの施錠、開錠を制御する。

- 5 後述するように、この実施形態では、家族構成員のそれぞれは、自分の電子鍵情報として、本鍵情報と、バックアップ鍵情報とを管理サーバ装置に登録することができる。電子鍵情報は、前述したように、電子鍵装置ごとに異なるので、本鍵情報とバックアップ鍵情報との登録は、本鍵装置と、バックアップ鍵装置との登録に等しい。
- 10 以下に説明する例においては、各人に与えられる本鍵装置としては、ドアロック制御システムの提供会社が提供する IC カードとされる。そして、この本鍵装置である IC カードの識別情報が、ドアロック制御システムが当該家に取り付けられる前に、予め管理サーバ装置に、当該 IC カードの所有者の電子鍵情報として登録される。
- 15 この場合に、この実施形態では、家族構成員の数分だけ、IC カードが前記提供会社から提供され、それらの複数の IC カードの全ての識別情報が、設置されるドアロック制御システム用の電子鍵情報として管理サーバ装置に登録される。
- 20 さらに、この実施形態では、管理サーバ装置には、ドアロック制御システムが設置される家の家族構成員のそれぞれについての個人情報が収集され、その個人情報に対応して、それぞれの家族構成員が持つ IC カードの識別情報が登録される。したがって、ドアロック制御システムは、電子鍵情報を検索することにより、それが誰の電子鍵情報であるかを判別することができる。つまり、この例の通信システムにおいては、電子
- 25 鍵情報を、家族構成員の個人識別情報として用いることが可能である。

そして、管理サーバ装置に登録された各家族構成員の本鍵情報は、ド

アロック制御システムが、当該家に設置された後、システムの設置事業者や、ユーザが管理サーバ装置に対して初期登録要求をすることにより、ドアロック装置の記憶部に登録され、電子鍵情報の認証用として使用されることになる。

- 5 また、この実施形態では、本鍵装置を紛失してしまった場合を考慮して、バックアップ鍵情報を登録しておくことができる。後述するように、この実施形態では、バックアップ鍵情報は、家族構成員の各人が、バックアップ鍵装置として使用したい電子鍵装置の識別情報（この例では、IC製造番号）を管理サーバ装置に登録することにより、登録可能である。
- 10 。

前述したように、この実施形態においては、電子鍵情報として用いる識別情報は、個人識別情報としても用いることができることを利用して、各家族構成員個々の玄関ドアからの入退出を管理することができるようにする。

- 15 このように電子鍵情報を個人識別情報としても用いることにより、当該家に住む家族構成員それぞれの玄関ドアからの入退出の管理をすることができ、帰宅予定者への帰宅時刻超過の通知や、子供の帰宅の状況の親への通知などを行なえると共に、前記入退出の情報を、セキュリティシステムに反映させることができ、より高機能のセキュリティシステムを構築することができる。
- 20 。

〔実施形態のドアロックシステムを含むセキュリティシステムの概要〕

図3は、ドアロック制御システムおよびセキュリティシステムを含む、この実施形態の通信システムの概要を説明するための図である。

- 25 家の玄関ドア1には、電子鍵装置と通信を行なうドアロック装置2が取り付けられている。室内には、セキュリティシステムを構成する監視制御装置3が設けられ、ドアロック装置2と接続されている。ドアロッ

ク装置 2 と監視制御装置 3 とは、この例では接続線により接続されるが、無線により接続するようにしてもよい。

監視制御装置 3 は、ドアロック装置 2 からの電子鍵情報を受け取って、前述した電子鍵情報の認証を行なう装置、つまり認証装置となることも
5 できる。しかし、この例では、電子鍵情報の認証は、ドアロック装置 2 自身において行なうようにされている。

そして、この例では、室内には、火災発生を検知する火災センサ 4 と、ガス漏れを検知するガスセンサ 5 と、窓の戸締りを検知する窓センサ 6 a, 6 b と、テレビ 7 が設けられ、それぞれ監視制御装置 3 に接続されて
10 ている。監視制御装置 3 とそれらとの接続も、接続線により接続されているが、無線により接続してもよい。

また、図 3 では省略したが、火災センサ 4 で火災発生を検知したときに、その発生現場近傍を撮影できるような位置や、窓センサ 6 a, 6 b で賊の侵入を検知したときに、その賊を撮影できるような位置には、監視
15 視カメラを設けるようにすることができる。その場合には、それら監視カメラは監視制御装置 3 に接続され、監視カメラの撮影画像が監視制御装置 3 に供給されるようにされる。

監視制御装置 3 は、また、電話回線 8 を通じ、通信ネットワーク 9 を通じてセキュリティシステムの管理会社が運営する管理サーバ装置 10
20 に接続される。この管理サーバ装置 10 も、ドアロック装置 2 からの電子鍵情報を、監視制御装置 3 を介して受け取ることにより、電子鍵情報の認証を行なう装置となることもできる。

通信ネットワーク 9 は、携帯電話網をも含み、後述するように、監視制御装置 3 は、異常状態の発生時に、予め登録された携帯電話端末 11 a, 11 b に、当該異常状態の発生を知らせることが可能とされている。
25 さらに、通信ネットワーク 9 は、インターネットを含み、パーソナルコ

ンピュータ 12 は、管理サーバ装置 10 に対して当該インターネットを通じてアクセスすることが可能とされている。また、携帯電話端末 11a, 11b から、管理サーバ装置 10 にアクセスすることが可能とされている。

- 5 なお、この実施形態においては、特許請求の範囲における制御装置は、ドアロック装置 2 の後述するドアロック制御装置と監視制御装置とで構成されるものである。

次に、ドアロック装置 2 の具体的構成例およびその動作、また、監視制御装置 3 の具体的構成例およびその動作について、詳細に説明する。

- 10 なお、以下に説明する例では、前述したように、電子鍵情報の認証は、ドアロック装置自身が行なうものとする。

[電子鍵装置の構成例]

前述したように、この実施形態においては、電子鍵装置としては、IC カードの他、携帯電話端末や PDA 端末なども用いることができる。

- 15 しかし、電子鍵装置は、生体情報の取得部と、制御用 IC チップと、通信手段とを備える点では共通している。電子鍵装置が IC カードである場合の構成例を次に示す。

<電子鍵装置の第 1 の例>

- 20 この第 1 の例の電子鍵装置は、生体情報として、指紋を用いる IC カードの場合の例である。図 4A は、この例の IC カード 40F の表面を示し、この表面には、所有者の氏名と、ID 番号が表示されていると共に、指紋読取部 41 の指紋読取窓 41W が形成されている。

- 25 また、図 4B は、IC カード 40F の内部構成例を示しており、IC カード 40F 内には、指紋読取部 41 と、後述するドアロック装置 2 の電子鍵リード／ライト部と通信を行なうための電磁誘導アンテナ 42 と、制御用 IC 43 と、情報送受信回路部 44 が内蔵されている。

指紋読取部 4 1 は、指紋読取窓 4 1 W に置かれた指の指紋を読み取り、その読み取った指紋の情報を制御用 I C 4 3 に送る。制御用 I C 4 3 は、予め登録されて記憶している I C カード 4 0 F の所有者の指紋情報と、読み取った指紋情報とを比較し、一致しているかどうか判別する。

5 そして、一致していると判別すると、予め制御用 I C 4 3 内のメモリに記憶されている電子鍵情報を読み出して、情報送受信回路部 4 4 および電磁誘導アンテナ 4 2 を通じて、外部に送出する。記憶している指紋情報と、読み取った指紋情報とを比較し、一致していないと判別したときには、電子鍵情報の外部への送出は禁止する。

10 図 5 は、第 1 の例の場合の I C カード 4 0 F の内部ブロック構成を示すものである。CPU (C e n t r a l P r o c e s s i n g U n i t) 4 0 1 に対してシステムバス 4 0 2 を介してプログラムやデータが記録されている ROM (R e a d O n l y M e m o r y) 4 0 3 と、ワークエリア用 RAM (R a n d o m A c c e s s M e m o r y) 4 0 4 と、電子鍵情報となる識別情報が記憶されている識別情報メモリ 4 0 5 と、通信履歴メモリ 4 0 6 と、送受信インターフェース 4 0 7 と、指紋登録メモリ 4 0 8 と、指紋読取部インターフェース 4 0 9 と、指紋照合部 4 1 0 とが接続されている。

20 識別情報メモリ 4 0 5 には、前述した I C 製造番号からなる識別情報が記憶されている。なお、この I C カード 4 0 の所有者の氏名、住所の他、所有者のその他の必要な個人情報を記憶することもできる。この個人情報は、父親、母親、子供などの区別が可能なように構成される。

25 通信履歴メモリ 4 0 6 には、各所有者が行ったドアロック装置 2 の後述する電子鍵リード／ライト部との通信の時刻や履歴（内側と外側のどちらの電子鍵リード／ライト部と通信したか情報を含む）や、各所有者の外出、帰宅の履歴などを書き込むことが可能とされている。なお、こ

これらの履歴情報は、後述するように、ドアロック装置 2 のメモリや監視制御装置 3 のメモリにおける家族構成員の各人に対応するエリアにも記憶されるものである。

送受信インターフェース 407 には、電磁誘導アンテナ 41 に接続されている情報送受信回路部 44 が接続されている。

指紋登録メモリ 408 には、当該 IC カード 40F の所有者の指紋の情報が予め登録されて記憶されている。指紋読取部インターフェース 409 は、指紋読取部 41 で読み取った指紋の情報を取り込むためのものである。指紋照合部 410 は、指紋読取部インターフェース 409 を通じて取得した指紋の情報と、指紋登録メモリ 408 から読み出した前記所有者の指紋の情報とを比較し、一致しているか否かを判定して、その判定結果をシステムバス 402 に送出する。指紋照合部 410 は、ハードウェアの構成ではなく、CPU 401 によるソフトウェアによる構成とすることもできる。

CPU 401 は、前述したように、指紋照合部 410 での判定結果に基づき、指紋一致、つまり、指紋照合が OK であったときには、識別情報メモリ 405 から読み出した識別情報からなる電子鍵情報を、送受信インターフェース 407、情報送受信回路 408 および電磁誘導アンテナ 41 を通じて送出し、指紋照合部 410 での判定結果が指紋不一致、つまり、指紋照合が NG であったときには、電子鍵情報の送出を禁止する。

また、CPU 401 は、電磁誘導アンテナ 42 にて受信した情報を、情報送受信回路部 44 および送受信インターフェース 407 を通じて取り込み、通信履歴メモリ 406 に書き込んだりする処理も行なう。

図 6 は、このときの CPU 401 での処理動作を説明するためのフローチャートである。

CPU 401は、指紋読取部インターフェース409を通じた指紋読取部41からの指紋情報の受信を待ち（ステップS1）、指紋情報を受信したと判別したときには、指紋登録メモリ408に登録されている所有者の指紋情報を読み出し、指紋照合部410において指紋照合を行な
5 わせる（ステップS2）。

そして、CPU 401は、指紋照合部410からの指紋照合の判定結果が指紋一致であるか否か判別し（ステップS3）、指紋不一致で照合がNGであったときには、処理をそのまま終了して、電子鍵情報の送
10 は行なわない。

また、CPU 401は、指紋一致で照合がOKであったときには、識別情報メモリ405から識別情報を読み出して、電子鍵情報として、情報送受信回路部44および電磁誘導アンテナ42を通じて送出する（ス
15 テップS4）。

そして、CPU 401は、相手方のリード／ライト部と通信を行なったか否か判別し（ステップS5）、電磁誘導アンテナ42、情報送受信回路部44および送受信インターフェース407を通じて相手方から所定の情報を受け取ったときには、相手方との通信を行なったとして、通信履歴を通信履歴メモリ406に書き込み（ステップS6）、その後、この処理ルーチンを終了する。
20

ステップS5で、相手方のリード／ライト部からの情報を受信せず、通信を行っていないと判別したときには、CPU 401は、電子鍵情報を送出してから予め定めた所定時間、経過したか否か判別し（ステップS7）、所定時間経過していないと判別したときには、ステップS4に戻り、電子鍵情報を再度送って相手方からの情報を待つ。そして、ステップS7で、所定時間経過したと判別したときには、この処理ルーチ
25 をそのまま終了する。

以上のように、この例の電子鍵装置としての I C カード 4 0 F によれば、予め登録してある所有者の指紋と、使用者の指紋とを照合して、照合が O K である場合にのみ電子鍵情報の送出を行なうので、予め登録された使用者しか、当該電子鍵装置を使用できず、もしも、当該電子鍵装置を紛失したとしても、他の使用者の使用を阻止することができる。

< 電子鍵装置の第 2 の例 >

この第 2 の例の電子鍵装置は、生体情報として、虹彩を用いる I C カードの場合の例である。図 7 A は、この例の I C カード 4 0 I の表面を示し、この表面には、所有者の氏名と、I D 番号が表示されていると共に、使用者の虹彩を読み取るための手段として、この例では、C C D (C h a r g e C o u p l e d D e v i c e) カメラ 4 5 が設けられている。

また、図 7 B は、I C カード 4 0 I の内部構成例を示しており、I C カード 4 0 I 内には、第 1 の例の I C カード 4 0 F と同様に、電磁誘導アンテナ 4 2 と、制御用 I C 4 3 と、情報送受信回路部 4 4 とが内蔵されていると共に、C C D カメラ 4 5 からの撮像信号を処理して制御用 I C 4 3 に供給するための撮像信号処理回路部 4 6 が内蔵されている。

使用者は、C C D カメラ 4 5 により自分の目（虹彩）を撮影させる。C C D カメラ 4 5 は、撮影した使用者の虹彩情報を撮像信号処理回路部 4 6 を通じて取り込み、その取り込んだ虹彩の情報を制御用 I C 4 3 に送る。制御用 I C 4 3 は、予め登録されて記憶されている I C カード 4 0 I の所有者の虹彩情報と、取り込んだ虹彩情報とを比較し、一致しているかどうか判別する。

そして、一致していると判別すると、予め制御用 I C 4 3 内のメモリに記憶されている電子鍵情報を読み出して、情報送受信回路部 4 4 および電磁誘導アンテナ 4 2 を通じて、外部に送出する。記憶している虹彩

情報と、取り込んだ虹彩情報とを比較し、一致していないと判別したときには、電子鍵情報の外部への送出手は禁止する。

図 8 は、第 2 の例の場合の I C カード 4 0 I の内部ブロック構成を示すものである。この第 2 の例においては、図 5 の第 1 の例の指紋登録メモリ 4 0 8 と、指紋読取部インターフェース 4 0 9 と、指紋照合部 4 1 0 とに代わって、虹彩情報登録メモリ 4 1 1 と、撮像信号インターフェース 4 1 2 と、虹彩照合部 4 1 3 とが設けられる。撮像信号インターフェース 4 1 2 は、C C D カメラ 4 5 に接続されている。その他の構成は、第 1 の例の図 5 と同様である。

10 虹彩情報登録メモリ 4 1 1 には、当該 I C カード 4 0 I の所有者の虹彩の情報が予め登録されて記憶されている。撮像信号インターフェース 4 1 2 は、撮像信号処理回路部 4 6 からの虹彩情報を取り込むためのものである。虹彩照合部 4 1 3 は、撮像信号インターフェース 4 1 2 を通じて取り込んだ虹彩情報と、虹彩情報登録メモリ 4 1 1 から読み出した
15 前記所有者の虹彩情報とを比較し、一致しているか否かを判定して、その判定結果をシステムバス 4 0 2 に送出する。虹彩照合部 4 1 3 は、ハードウェアの構成ではなく、C P U 4 0 1 によるソフトウェアによる構成とすることもできる。

C P U 4 0 1 は、虹彩照合部 4 1 3 での判定結果に基づき、虹彩一致、
20 つまり、虹彩照合が O K であったときには、識別情報メモリ 4 0 5 から読み出した識別情報からなる電子鍵情報を、送受信インターフェース 4 0 7 、情報送受信回路 4 4 および電磁誘導アンテナ 4 1 を通じて送出し、虹彩照合部 4 1 3 での判定結果が虹彩不一致、つまり、虹彩照合が N G であったときには、電子鍵情報の送出手を禁止する。

25 図 9 は、このときの C P U 4 0 1 での処理動作を説明するためのフローチャートである。

CPU 401は、撮像信号インターフェース412を通じた撮像信号処理回路部46からの虹彩情報の受信を待ち（ステップS11）、虹彩情報を受信したと判別したときには、虹彩情報登録メモリ411に登録されている所有者の虹彩情報を読み出し、虹彩照合部413において虹彩照合を行なわせる（ステップS12）。

そして、CPU 401は、虹彩照合部413からの虹彩照合の判定結果が虹彩一致であるか否か判別し（ステップS13）、虹彩不一致で照合がNGであったときには、処理をそのまま終了して、電子鍵情報の送出手は行なわない。

10 また、CPU 401は、虹彩一致で照合がOKであったときには、識別情報メモリ405から識別情報を読み出して、電子鍵情報として、情報送受信回路部44および電磁誘導アンテナ42を通じて送出する（ステップS14）。

そして、CPU 401は、相手方のリード／ライト部と通信を行なったか否か判別し（ステップS15）、電磁誘導アンテナ42、情報送受信回路部44および送受信インターフェース407を通じて相手方から所定の情報を受け取ったときには、相手方との通信を行なったとして、通信履歴を通信履歴メモリ406に書き込み（ステップS16）、その後、この処理ルーチンを終了する。

20 ステップS15で、相手方のリード／ライト部からの情報を受信せず、通信を行っていないと判別したときには、CPU 401は、電子鍵情報を送出してから予め定めた所定時間、経過したか否か判別し（ステップS17）、所定時間経過していないと判別したときには、ステップS14に戻り、電子鍵情報を再度送って相手方からの情報を待つ。そして、
25 ステップS7で、所定時間経過したと判別したときには、この処理ルーチンをそのまま終了する。

以上のように、この第2の例の電子鍵装置としてのICカード40Iによれば、予め登録してある所有者の虹彩と、使用者の虹彩とを照合して、照合がOKである場合にのみ電子鍵情報の送出を行なうので、予め登録された使用者しか、当該電子鍵装置を使用できず、もしも、当該電子鍵装置を紛失したとしても、他の使用者の使用を阻止することができる。

[生体情報の他の例]

以上の例では、生体情報としては、指紋と、虹彩の場合について説明したが、生体情報としては、これに限られるものではない。例えば手の甲の静脈パターンを生体情報として用いることもできる。この場合には、虹彩情報に代えて、所有者の手の甲の静脈パターンを登録して記憶しておくとともに、CCDカメラ45により、手の甲の静脈パターンを撮影して取り込むことにより、第2の例のICカード40Iの構成をそのまま用いることができる。

なお、以上の例に限らず、個人識別が可能な生体情報であって、所定の手段により取得可能なものであれば、どのような生体情報も、利用することができることは勿論である。

[ドアロック装置の構成]

図10Aおよび図10Bは、ドアロック装置2の構成例を説明するための図である。図10Aは、家の外側から玄関ドア1のドアロック装置2の取り付け部分近傍を見た図である。また、図10Bは、玄関ドア1のドアロック装置2の取り付け部分近傍を、玄関ドア1の端面側から見た図である。

この例のドアロック装置2においては、玄関ドア1の外側（戸外側）には、電子鍵装置の例としてのICカード40Fや40Iと通信を行なうための外側電子鍵リーダー/ライタ部21exと、電子鍵情報の認証結

果や玄関ドア 1 の施錠または開錠を視覚的に知らせるための表示素子の例としての外側 LED (Light Emitting Diode; 発光ダイオード) 22 ex と、電子鍵情報の認証結果や玄関ドア 1 の施錠または開錠を音声により知らせるための外側スピーカ 23 ex と、外側ドアノブ 24 ex とが設けられている。

また、玄関ドア 1 の内側 (屋内側) にも、電子鍵装置の例としての IC カード 40 F や 40 I と通信を行なうための内側電子鍵リーダ/ライタ部 21 in と、電子鍵情報の認証結果や玄関ドア 1 の施錠または開錠を視覚的に知らせるための表示素子の例としての内側 LED 22 in と、電子鍵情報の認証結果や玄関ドア 1 の施錠または開錠を音声により知らせるための内側スピーカ 23 in と、内側ドアノブ 24 in とが設けられている。

玄関ドア 1 には、さらに、玄関ドア係止片 25 と、ロック片 26 と、ドア開閉センサ 27 が設けられている。さらに、玄関ドア 1 の内側には、ドアロック装置 2 の動作を制御するためのドアロック制御装置 100 が設けられており、電子鍵リーダ/ライタ部 21 ex および 21 in、LED 22 ex および 22 in、スピーカ 23 ex および 23 in、ドア開閉センサ 27 および図示を省略したドアロック機構駆動部が、このドアロック制御装置 100 に接続されている。

玄関ドア係止片 25 は、ドアノブ 24 ex あるいはドアノブ 24 in の操作に応じて、玄関ドアの端面 1 a に垂直な方向に摺動移動する部材である。これは、後述するオートロックモードでない場合において、玄関ドア 1 が施錠されていないときにも、玄関ドア 1 の端面 1 a と対向する壁の端面側に設けられる凹部に勘合して、玄関ドア 1 を、係止するためのものである。

ロック片 26 は、ドアロック機構の一部を構成する部材であり、図 1

0 Aおよび図 1 0 Bでは図示を省略したドアロック機構駆動部によりドアロック機構が駆動されることにより、玄関ドアの端面 1 aに垂直な方向に摺動移動して、玄関ドア 1を施錠するときには、図 1 0 Aのように、玄関ドア 1の端面 1 aから突出する状態に固定され、玄関ドア 1を開錠するときには、玄関ドア 1の端面 1 aから突出しない状態に固定される。

5 なお、図示は省略したが、玄関ドア 1の端面 1 aと対向する壁の端面には、このロック片 2 6が突出した状態のときに嵌合される凹部が形成されており、ロック片 2 6が当該凹部に嵌合される状態が玄関ドアの施錠状態となる。そして、ロック片 2 6が玄関ドア 1側に引っ込んで、当該凹部に嵌合していないときには、施錠状態が解除されて、開錠状態になる。

10 玄関ドア開閉センサ 2 7は、例えば光学式センサが用いられ、玄関ドア 1が開けられたときは外部光を検知することにより、それを検知し、玄関ドア 1が閉じられたときには、玄関ドア 1の端面 1 aが、壁の端面と衝合することにより外部光が遮断されることを検知することにより、それを検知して、玄関ドア 1の開閉を検知する。

[ドアロック制御装置 1 0 0の説明]

次に、ドアロック制御装置 1 0 0を中心にしたドアロック装置 2の電氣的な構成例を図 1 1に示す。なお、以下の説明においては、電子鍵装置としては、指紋照合認証を行なう第 1の例の I Cカード 4 0 Fを用いるものとする。

すなわち、ドアロック制御装置 1 0 0は、マイクロコンピュータの構成を備えており、CPU (C e n t r a l P r o c e s s i n g U n i t) 1 0 1に対してシステムバス 1 0 2を介してプログラムやデータが記録されているROM (R e a d O n l y M e m o r y) 1 0 3と、ワークエリア用RAM (R a n d o m A c c e s s M e m o

ry) 104と、家族構成員の個々についての電子鍵情報となる識別情報（この例では、IC製造番号）が記憶されている家族情報メモリ120と、監視制御装置3と通信を行なうための通信インターフェース121と、時計回路122が接続されている。

- 5 家族情報メモリ120には、後述するように、管理サーバ装置10に登録された本鍵情報やバックアップ鍵情報が、家族構成員のそれぞれについて、電子鍵情報として登録されて格納されている。また、各家族構成員を識別するための情報、例えば、氏名、年齢、性別、続き柄、その他の個人情報も、併せて家族情報メモリ120に格納するようにしても
- 10 よい。この家族情報メモリ120への電子鍵情報の登録に関しては、後述する。

- また、システムバス102には、インターフェース105および106を介して内側電子鍵リード／ライト部21inおよび外側電子鍵リード／ライト部21exが接続され、また、内側LED駆動部107を介して内側LED22inが接続され、外側LED駆動部108を介して外側LED22exが接続され、さらに、音声出力インターフェース109を介して内側スピーカ23inが接続され、音声インターフェース110を介して外側スピーカ23exが接続される。
- 15

- さらに、システムバス102には、インターフェース111を介して
- 20 ドア開閉センサ27が接続されると共に、ドアロック機構駆動部112を介して、ロック片26を摺動駆動させるドアロック機構28が接続される。

- 電子鍵リード／ライト部21exまたは21inは、ICカード40F（または40I）と通信を行なう通信部を構成する。電子鍵リード／
- 25 ライト部21exまたは21inは、この例では、電磁誘導アンテナおよび情報送受信部を含む。

この例のドアロック制御装置100は、ドアロック制御モードとして、オートロックモードと、逐次ロックモードとの2通りの制御モードを備えている。

オートロックモードは、ドアロック制御装置100が、電子鍵リード／ライト部21ex, 21inを介してICカード40Fと通信することに基づき玄関ドア1を開錠した後、所定時間後に自動的に玄関ドアを施錠状態にするモードである。オートロックモードにおいては、常に、内側と外側の電子鍵リード／ライト部21ex, 21inの両方を用いるものとなる。

また、逐次ロックモードは、少なくとも玄関ドア1の外側の電子鍵リード／ライト部21exを通じてICカード40Fと通信することに基づき玄関ドアの施錠、開錠の状態を、そのときの状態とは逆の状態にするモードである。この逐次ロックモードにおいても、内側と外側の電子鍵リード／ライト部21ex, 21inの両方を用いることができるが、内側は、別途のマニュアルの施錠手段により施錠するようにした場合には、外側の電子鍵リード／ライト部21exを通じたICカード40Fとの通信のみにより、玄関ドアの施錠、開錠動作を行なわせるようにすることができる。この逐次ロックモードは、従来からの一般的な鍵による施錠、開錠の方法に合わせたモードである。

ドアロック装置2のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、この例では、例えば、ドアロック装置2を取り付ける際に、後述するように、作業者により監視制御装置3を通じて行なわれる。

ドアロック装置2がいずれのドアロック制御モードに設定されているかの情報は、ドアロック制御装置100内の図示を省略した不揮発性メモリに格納されており、ドアロック制御装置100は、当該不揮発性メ

モリの記憶情報を参照することにより、自装置のドアロック制御モードが、オートロックモードか、逐次ロックモードかを認識するものである。監視制御装置 3 を通じたドアロック制御モードの設定動作に関しては、後述する。

- 5 なお、ドアロック装置 2 のドアロック制御モードをオートロックモードとするか、逐次ロックモードとするかの選択設定は、監視制御装置 3 を通じて行なうのではなく、ドアロック装置 2 に直接的に行なうようにすることもできる。例えば、予め、ドアロック装置 2 の出荷時に、いずれのドアロック制御モードにするかの設定をドアロック装置 2 に行な
- 10 ておくようにしても良い。また、ドアロック装置 2 に、ドアロック装置 2 の設置作業者が操作可能な入力操作手段、例えばディップスイッチ等を設けておき、当該入力操作手段を通じて、ドアロック制御モードの設定を行なうようにしてもよい。

〔監視制御装置 3 の外観の説明〕

- 15 図 1 2 は、室内に設けられるセキュリティシステム用の監視制御装置 3 の構成を説明するための外観図であり、この監視制御装置 3 は、例えば赤外線や電波を用いたリモートコマンド 5 0 によりリモコン制御可能の構成とされている。

- 20 監視制御装置 3 の筐体 3 0 には、ビデオカメラ 3 1 が組み込まれている。このビデオカメラ 3 1 は、この例では、実線位置の横置き状態と、点線位置の縦置き状態とのいずれの状態をも取れる機構により、筐体 3 0 に対して取り付けられている。このビデオカメラ 3 1 は、セキュリティモードがオンとされたときに、監視制御装置 3 からの指示により撮影を開始するようにされている。

- 25 また、ビデオカメラ 3 1 による撮影方向は、ビデオカメラが首振り方向に調整可能な構造とされているので、その調整により変えられるよう

にされている。したがって、使用者は、セキュリティモードオンに先立ち、ビデオカメラ 3 1 による撮影方向の調整を行なっておくことができる。

そして、筐体 3 0 には、ビデオカメラ 3 1 による撮影対象部を明るく
5 照明するための撮影用ランプ 3 2 が設けられている。また、筐体 3 0 には、例えば遠赤外線を検知することにより人を検知する人感センサ 3 3 が設けられている。監視制御装置 3 は、後述するように、セキュリティモードオンのときに人感センサ 3 3 で人を検知したときには、賊の侵入
10 であるとして検知し、撮影用ランプ 3 2 をオンにすると共に、所定の通報先に撮影画像を送るようにする。

筐体 3 0 には、また、マイクロホン 3 4 とスピーカ 3 5 とが設けられている。マイクロホン 3 4 は、賊の声や賊侵入時の室内の臨場音を收音するためのものである。スピーカ 3 5 は、侵入してきた賊を威嚇する音声を放音するためなどに用いられる。

15 筐体 3 0 には、また、電子鍵リード／ライト部 3 6 が設けられる。この電子鍵リード／ライト部 3 6 は、この例では、伝言の記録、再生の際に用いられる。すなわち、この例においては、監視制御装置 3 は、伝言装置の役割もできるように構成されており、電子鍵リード／ライト部 3 6 により、電子鍵装置としての I C カード 4 0 F を読み取らせた後、後
20 述するようにリモートコマンド 5 0 の伝言記録ボタンを押すと、設定した相手（家族の誰か）に伝言が残すことができ、また、リモートコマンド 5 0 の伝言再生ボタンを押すと、自分宛ての伝言を再生することができるようになっている。

この伝言が記録されているかどうかなどを知らせるため等の用途として、
25 筐体 3 0 には、複数個の L E D 3 7 が設けられている。また、筐体 3 0 には、さらに、リモートコマンド 5 0 からのリモコン信号の受信部

38が設けられる。

また、図12では図示を省略したが、監視制御装置3の背面パネルには、テレビ受像機7のビデオ入力端子に接続される映像出力端子が設けられている。そして、監視制御装置3には、テレビ受像機7の電源のオン・オフなどを制御するためのリモコン送信部39が設けられている。

さらに、監視制御装置3は、火災センサ4、ガスセンサ5、窓センサ6a、6b、さらには、監視カメラを接続するためのセンサハブを備えている。また、図3で説明したように、監視制御装置3は、電話回線を通じて、セキュリティシステムの管理会社が運営する管理サーバ装置10にアクセスできるように構成されている。

[監視制御装置3の構成例]

監視制御装置3の内部構成および監視制御装置3と周辺機器との接続状態の構成例を図13に示す。

監視制御装置3は、マイクロコンピュータの構成を備えており、CPU201に対して、システムバス202を介して、プログラムやデータが記録されているROM203と、ワークエリア用RAM204と、ドアロック制御装置100の家族情報メモリ120と同様に、電子鍵装置としてのICカード40Fまたは40Iを所有する家族全員の電子鍵情報となる識別情報が記憶されている家族情報メモリ205と、ドアロック制御装置100と通信を行なうためのドアロック装置通信インターフェース206と、センサハブ207と、ビデオカメラ31の撮影画像およびマイクロホン34で収音した音声を記憶するための画像・音声メモリ208と、電話回線を通じて管理サーバ装置10等と通信を行なうための通信インターフェース209とが接続されている。

また、システムバス202には、カメラインターフェース210を介してビデオカメラ31が、インターフェース211を介して撮影用ラン

プ 3 2 の照明機構 3 2 0 が、インターフェース 2 1 2 を介して人感セン
サ 3 3 が、インターフェース 2 1 4 を介して電子鍵リード／ライト部 3
6 が、インターフェース 2 1 5 を介してリモコン受信部 3 8 が、インタ
ーフェース 2 1 6 を介してリモコン送信部 3 9 が、音声入力インターフ
ェース 2 1 8 を介してマイクロホン 3 4 が、インターフェース 2 1 9 を
介して LED 3 7 が、音声出力インターフェース 2 2 0 を介してスピー
カ 3 5 が、それぞれ接続されている。

さらに、システムバス 2 0 2 は、ビデオ信号出力端子からなるテレビ
インターフェース 2 1 7 を介してテレビ受像機 7 に接続されている。ま
た、システムバス 2 0 2 には、時計回路 2 2 1 と、通知連絡設定メモリ
2 2 2 とが接続されている。

家族情報メモリ 2 0 5 は、例えば EEPROM (E l e c t r i c a
l l y E r a s a b l e P r o g r a m m a b l e R O M) で構
成される。

家族情報メモリ 2 0 5 には、ドアロック制御装置 1 0 0 の家族情報メ
モリ 1 2 0 と同様に、家族構成員のそれぞれについての識別情報と、個
人情報とが格納されている。この明細書では、識別情報と個人情報と
からなる情報を、個人プロフィール情報と呼ぶことにする。

後述するように、この例では、家族構成員すべての個人プロフィール
情報は、ドアロック装置 2 および監視制御装置 3 が設置されたときに、
設置管理者が管理サーバ装置 1 0 に初期登録依頼をすることにより、管
理サーバ装置 1 0 から送られてきて、監視制御装置 3 に自動的に登録さ
れる。そして、監視制御装置 3 は、少なくとも個人プロフィール情報の
うちの個人識別情報を電子鍵情報として、ドアロック制御装置 1 0 0 に
転送する。ドアロック制御装置 1 0 0 は、その電子鍵情報を家族情報メ
モリ 1 2 0 に登録する。

図 1 4 に、一人分の個人プロフィール情報の例を示す。図 1 4 に示すように、個人プロフィール情報は、個人識別情報と個人情報とが対応付けられて記憶された情報である。この実施形態では、個人識別情報は、前述したように、電子鍵装置の各メモリに格納されている識別情報が用いられる。個人識別情報は個人情報と対応させることで、具体的に誰の識別情報であるかが判明する。この識別情報は、電子鍵情報の役割を有することは前述した通りであり、図 1 4 に示すように、電子鍵情報としては、本鍵情報とバックアップ鍵情報とが登録可能である。バックアップ鍵情報は、複数個、登録可能としてもよい。

図 1 4 の例においては、個人情報としては、個人識別情報以外の情報であり、パスワード情報、氏名、住所、生年月日、年齢、続柄、登録日、銀行口座番号、電話番号、電子メールアドレス、IP アドレス、趣味／嗜好情報、家の玄関 8 からの入退出履歴情報、電子鍵登録・紛失履歴情報などが家族情報メモリ 2 0 5 に記憶される。

この例の入退出履歴情報には、外出時刻、帰宅時刻が記憶されるほか、外出中であるか、在宅であるかの在／不在フラグが含まれる。この入退出履歴情報は、監視制御装置 3 が玄関ドア 7 を通じての家族の入退出を管理するために用いられる。また、電子鍵登録・紛失履歴情報は、後述するように、管理サーバ装置 1 0 からの電子鍵情報のバックアップ登録要求や抹消要求が到来して、バックアップ登録や抹消処理をしたときに、その日付、時刻とともに、バックアップ鍵情報や抹消した電子鍵情報を、バックアップ登録および抹消の区別をして記録しておくものである。

さらに、この例では、この家族情報メモリ 2 0 5 には、セキュリティモード用の情報も格納されている。すなわち、この例では、監視制御装置 3 では、家族構成員の在宅状況に応じて、セキュリティレベルを変更することが可能なように構成されている。図 1 5 は、セキュリティレベ

ルと家族構成員の在宅状況との関係を示すテーブルである。また、図 1 6 は、セキュリティレベルとセキュリティ内容との対応を示すテーブルである。

図 1 6 に示すように、この例においては、セキュリティレベルは、セキュリティレベルが高い方から順に、レベル A、レベル B、レベル C、レベル D まであり、レベル A においては、窓および玄関ドアの監視、火災やガス漏れの監視、ビデオカメラ 3 1 による監視の全てを行ない、レベル B では、ビデオカメラ 3 1 による監視は行なわずに、窓および玄関ドアの監視および火災やガス漏れの監視を行ない、レベル C では、火災やガス漏れの監視のみを行ない、レベル D では、監視を行なわない、という内容である。

そして、図 1 5 に示すように、家族構成員の在宅状況のそれぞれに対して各セキュリティレベルが割り付けられる。すなわち、この例では、父親が在宅の状況では、監視を行なわないレベル D とされる。また、父親が不在であるが母親が在宅の状況では、火災やガス漏れの監視のみを行なうレベル C とされる。また、子供のみが在宅の状況では、窓および玄関ドアの監視および火災やガス漏れの監視を行なうレベル B とされる。そして、全員が不在である状況では、全ての監視を行なうレベル A とされる。

監視制御装置 3 では、セキュリティモードをオンにするとき、また、セキュリティレベルを変更するとき、これら図 1 5、図 1 6 のテーブルを参照し、在宅状況に応じてセキュリティレベルを決定するようにする。

図 1 5 のセキュリティレベルと、家族構成員の在宅状況との関係は、予め設定しておくこともできるし、使用者が、例えばリモートコマンド 5 0 を用いて監視制御装置 3 に入力設定することにより、設定を変更することができるように構成されている。

なお、これら図 1 5、図 1 6 のテーブル情報は、家族情報メモリ 2 0 5 ではなく、別のメモリに格納するようにしても良いことは言うまでもない。

5 ドアロック装置通信インターフェース 2 0 6 は、ドアロック制御装置 1 0 0 に接続されている。センサハブ 2 0 7 には、火災センサ 4、ガスセンサ 5、窓センサ 6 a, 6 b および 1 個あるいは複数個の監視カメラ 1 3 が接続される。

10 画像・音声メモリ 2 0 8 は、セキュリティモードがオンであるときに、ビデオカメラ 3 1 で撮影した画像情報と、マイクロホン 3 4 で収音した音声情報とをバッファリングする監視情報領域と、伝言として記録されている画像情報および音声情報を記憶する伝言情報領域とを備えている。また、監視情報領域には、監視カメラ 1 3 用の画像記憶領域も設けられている。

15 監視情報領域は、この例では、所定時間、例えば 3 0 秒分の画像情報および音声情報を、いわゆるリングバッファ形式で記憶する。なお、監視情報領域と伝言情報領域とは、別々のメモリの構成とすることも勿論できる。

20 通信インターフェース 2 0 9 は、この例では、ルータ 6 1 に接続されている。ルータ 6 1 は、ADSL モデム 6 2、スプリッタ 6 3 を通じて電話回線 6 5 に接続されている。スプリッタ 6 3 には、電話端末 6 4 が接続される。

時計回路 2 2 1 は、現在時刻の情報をシステムバス 2 0 2 に送出する。現在時刻の情報には、年、月、日、曜日などのいわゆるカレンダー情報も含む。

25 通知連絡設定メモリ 2 2 2 は、後述するように、使用者により、リモートコマンド 5 0 が用いられて設定された帰宅予定者、外出予定者、帰

宅予定時刻、外出予定時刻、通知連絡者などの設定情報を記憶する。CPU 201は、この設定情報に基づいて、設定された通知連絡者に、帰宅予定者や外出予定者の帰宅状況や帰宅時刻、外出状況や外出時刻などを通知連絡するようにする。設定動作や通知連絡の動作に関しては、後述する。

[リモートコマンド50の説明]

監視制御装置3用のリモートコマンド50は、図12に示すように、セキュリティボタン51と、オフボタン52と、伝言記録ボタン53と、伝言再生ボタン54と、メニューボタン55と、上下左右の選択を行なう4個のキーとその中央の決定キーとからなるカーソルボタン56とを備えて構成されている。

メニュー項目としては、この例では、管理サーバ装置10に対する電子鍵情報としての個人IDの登録、ドアロック装置2のドアロック制御モードの設定、その他が、用意されており、それぞれのメニュー項目に対応する処理を実行するアプリケーションプログラムは、監視制御装置3のROM 203に格納されている。

[管理サーバ装置10の構成]

次に、管理サーバ装置10の構成例を図17に示す。管理サーバ装置10は、コンピュータの構成を備えており、CPU 301に対して、システムバス302を介して、プログラムやデータが記録されているROM 303と、ワークエリア用RAM 304と、ドアロック装置管理データベース305と、電子鍵登録・紛失履歴メモリ306と、インターネットなどの通信ネットワークを通じて通信を行なうための通信インターフェース307とが接続されている。また、システムバス302には、さらに、ホームページ用メモリ308と、画像・音声メモリ309とが接続されている。

ドアロック装置管理データベース 305 には、ドアロック装置 2 および監視制御装置 3 のシリアル番号、ドアロック装置 2 および監視制御装置 3 が設置された住所、電話番号、IP アドレス、ドアロック装置の利用者の氏名、登録された電子鍵情報を個人プロフィール情報など、
5 ロック装置 2 の管理に必要な事項が格納されている。電話番号、IP アドレスは、ドアロック装置 2 および監視制御装置 3 の通信ネットワーク 9 上のアドレス情報である。

電子鍵登録・紛失履歴メモリ 306 には、各ドアロック装置 2 ごとに、電子鍵情報の登録と紛失の履歴が記憶される。ホームページ用メモリ 3
10 08 には、ホームページの各ページの表示情報が格納されており、CPU 301 の指示に従い、必要なページの表示情報が、このメモリ 308 から読み出されて、通信インターフェース 307 を通じて通信ネットワークに送出される。

画像・音声メモリ 309 は、後述するように、セキュリティ監視システムから送られてくる画像・音声情報を格納する。管理サーバ装置 10
15 では、セキュリティ監視システムからの画像・音声をチェックして、警備会社に通知したり、ユーザの求めに応じて、画像・音声情報をホームページを通じて提供するようにする。

次に、以上のような構成の通信システムにおける種々の動作について、
20 以下に説明する。

[監視制御装置 3 における伝言記録および伝言再生；図 18]

前述したように、この例の監視制御装置 3 は、電子鍵装置、この例では IC カード 40F と、リモートコマンド 50 を用いて、特定の家人を指定して、伝言を記録しておくことができる。伝言が監視制御装置 3 に
25 記録されているときには、LED 37 が点灯あるいは点滅して、その旨を知らせるようにしている。

そして、監視制御装置 3 に、伝言が記録されている場合には、帰宅した家人が、自分の電子鍵装置としての IC カード 40 F を、この電子鍵リード／ライト部 36 により読み取らせ、リモートコマンド 50 により伝言再生を指示すると、記録されている伝言が、その人宛ての伝言である場合には、監視制御装置 3 は、記録されている伝言を、テレビ受像機 7 やスピーカ 35 を通じて再生するようにするように構成されている。

図 18 は、この伝言記録および再生のための監視制御装置 3 の処理を説明するためのフローチャートである。この図 18 の各ステップ S の処理は、CPU 201 が ROM 203 に記憶されているプログラムにしたがって実行されるものである。

すなわち、まず、使用者は、伝言記録または伝言再生をするには、自分の IC カード 40 F を電子鍵リード／ライト部 36 にかざして、通信を行なうようにする。CPU 201 は、電子鍵リード／ライト部 36 で IC カード 40 F と通信が行なわれたか否か判別し(ステップ S 21)、通信が行われたと判別すると、受信した識別情報により、誰の IC カード 40 F と通信したかを認識する(ステップ S 22)。

次に、リモートコマンド 50 からのリモコン信号の到来を待ち(ステップ S 23)、リモコン信号を受信したことを確認したら、そのリモコン信号は、伝言記録ボタン 53 の操作によるものか否か判別し(ステップ S 24)、伝言記録ボタン 53 の操作によるものであると判別したときには、CPU 201 は、伝言記録動作を行なうようにする(ステップ S 33)。

この伝言記録動作においては、監視制御装置 3 は、ビデオカメラ 31 で撮影された伝言者の画像情報をカメラインターフェース 210 を介して取り込み、画像・音声メモリ 208 の伝言記録領域に格納すると共に、マイクロホン 34 で収音した伝言音声情報(伝言メッセージ)をインタ

一フェース 218 を通じて取り込み、画像・音声メモリ 208 の伝言記録領域に格納する。このとき、それら画像情報および音声情報は、電子鍵装置 40 から読み込んだ識別情報に対応付けられて、当該識別情報と共に画像・音声メモリ 208 に格納される。

- 5 次に、CPU 201 は、家族情報メモリ 208 に記憶されている家族の個人プロフィール情報を参照して、伝言記録をしようとしている操作者以外の伝言相手のリストをテレビ受像機 7 の画面に表示する（ステップ S 34）。このとき、テレビ受像機 7 に電源が投入されていないときには、リモコン送信部 38 を通じて電源をオンにするリモコン信号をテレビ受像機 7 に供給して、テレビ受像機 7 に電源を投入しておく。なお、
10 伝言相手のリストの画面は、例えばスーパーインポーズによりテレビ番組の画像に重ねて表示するようにしてもよいし、テレビ番組の画像に重ねることなく単独の画面としてもよい。

- 15 操作者は、この伝言相手のリストから、リモートコマンド 50 のカーソルキー 56 を用いて、伝言相手の選択入力を行ない、カーソルキー 56 中の中央の決定キーを押す。監視制御装置 3 の CPU 201 は、この伝言相手の選択入力を受信して（ステップ S 35）、当該伝言相手の情報を、画像・音声メモリ 208 の伝言記録領域の、前記画像情報および伝言音声メッセージに対応させて格納して登録する（ステップ S 36）。
20 そして、伝言が記録されたことを報知するために、1 個の LED 37 を点灯させる（ステップ S 37）。LED 37 は、図 12 に示したように複数個設けられており、記録されている伝言の数だけ、点灯することとなる。

- 25 また、ステップ S 24 において、リモコン信号が伝言記録ボタン 53 の操作によるものではないと判別したときには、伝言再生ボタン 54 の操作によるものであるか否かを判別する（ステップ S 25）。伝言再生ボ

タン54の操作によるものでないと判別したときには、CPU201は、当該操作されたボタンに応じた処理を行なう（ステップS26）。

そして、ステップS25において、伝言再生ボタン54の操作によるものであると判別したときには、CPU21は、ステップS22で認識した識別情報を検索子として、画像・音声メモリ208の伝言記録領域の記憶内容を検索して、ICカード40Fを電子鍵リード／ライト部36にかざした操作者宛ての伝言があるか否か判別する（ステップS27）。

そして、ステップS27において、操作者宛ての伝言が無いと判別したときには、CPU201は、例えば予めROM203に用意されている「伝言はありません」の文字情報をテレビ受像機7の画面に表示すると共に、スピーカ35を通じて音声として放音して、操作者に報知する（ステップS28）。

また、ステップS27において、操作者宛ての伝言が有ると判別したときには、当該操作者宛ての伝言画像および伝言音声を画像・音声メモリ208から読み出して、テレビ受像機7に表示すると共に、スピーカ35から放音して再生する（ステップS29）。

伝言の再生が終了すると、CPU201は、テレビ受像機7の画面に伝言を消去するかどうかの問い合わせを表示するので、操作者は、その表示画面に含まれる「YES」、「NO」のいずれかをリモートコマンド50のカーソルキー56を用いて選択する。CPU201は、当該操作者の選択入力から、伝言を消去するか否か判別し（ステップS30）、消去すると判別したときには、画像・音声メモリ208の対応する画像・音声情報を消去し（ステップS31）、点灯しているLED37の一つを消灯する（ステップS32）。そして、この伝言記録再生処理ルーチンを終了する。

また、ステップS30で、伝言を消去しないと判別したときには、そ

のまま、この伝言記録再生処理ルーチンを終了する。

[ドアロック制御モードの選択設定；図19、図20]

前述したように、この実施形態では、監視制御装置3を通じてドアロック制御モードの設定ができるようにされているので、その設定動作を、
5 図19のフローチャートを参照しながら説明する。

まず、監視制御装置3のCPU201は、リモコン受信部38の受信信号を監視して、ドアロック制御モードの設定を含む設定メニューのための特定のボタン操作がなされたか否か判別する（ステップS41）。この例では、この特定のボタン操作としては、通常の利用者が行なわな
10 い操作とされており、例えばセキュリティボタン51とメニューボタン55との同時操作などとされている。このような特定のボタン操作は、ドアロック装置2の設置業者等が設定作業を行なうために定義されている。簡単に、ドアロック制御モードの設定変更ができないようにするためである。

15 ステップS41で、前記の特定のボタン操作はされないと判別されたときには、単独のボタン操作に応じた処理などの、その他の処理を行なう（ステップS42）。また、ステップS41で、前記の特定のボタン操作がされたと判別されたときには、設定メニューの一覧をテレビ受像機7の画面に、前述の伝言記録再生の場合と同様にして表示するように
20 する（ステップS43）。

この設定メニューの一覧表示に対しては、操作者は、行ないたい設定メニュー項目の選択をリモートコマンド50のカーソルキーを用いて行なう。CPU201は、リモコン受信部38の受信信号を監視してメニュー項目の選択操作がなされたか否か判別し（ステップS44）、メ
25 ニュー項目の選択操作がなされたと判別したときには、例えば反転表示して示す選択中項目を、選択操作に応じて変更する（ステップS45）。

そして、設定項目の決定操作がなされたか否か判別する（ステップ S 4 6）。また、ステップ S 4 4 で、メニュー項目の選択操作がなされないと判別したときには、即座にステップ S 4 6 に進んで設定項目の決定操作がなされたか否か判別する。

- 5 ステップ S 4 6 で、設定項目の決定操作がなされないと判別したときには、ステップ S 4 4 に戻る。また、ステップ S 4 6 で、設定項目の決定操作がなされたと判別したときには、選択された設定項目はドアロック制御モードの設定であるか否か判別し（ステップ S 4 7）、そうではなかったときには選択された他の設定項目についての処理ルーチンを実行する（ステップ S 4 8）。

- 10 ステップ S 4 7 で、選択された設定項目はドアロック制御モードの設定であると判別したときには、CPU 2 0 1 は、テレビ受像機 7 の画面にオートロックモードと、逐次ロックモードとの選択画面を表示する（ステップ S 4 9）。操作者は、この選択画面において、いずれかの選択入力
- 15 力をカーソルキー 5 6 を用いて行なう。

そこで、CPU 2 0 1 は、リモコン受信部 3 8 を監視して、オートロックモードが選択されたか否か判別し（ステップ S 5 0）、オートロックモードが選択されたと判別したときには、ドアロック装置 2 をオートロックモードに設定する設定動作を行なう（ステップ S 5 1）。

- 20 すなわち、CPU 2 0 1 は、監視制御装置 3 に内蔵の不揮発性メモリ部のドアロック装置 2 のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶すると共に、オートロックモードにする旨の指示をドアロック装置 2 に対して、ドアロック装置通信インターフェース 2 0 6 を通じて送る。

- 25 また、ステップ S 5 0 で、オートロックモードではないと判別したときには、CPU 2 0 1 は、逐次ロックモードが選択されたと判別して、

ドアロック装置 2 を逐次ロックモードにする設定動作を行なう（ステップ S 5 2）。

すなわち、CPU 2 0 1 は、監視制御装置 3 に内蔵の不揮発性メモリ部のドアロック装置 2 のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶すると共に、逐次ロックモードにする旨の指示をドアロック装置 2 に対して、ドアロック装置通信インターフェース 2 0 6 を通じて送る。

以上で、監視制御装置 3 におけるロック制御モードの設定時の動作は終了となる。

10 次に、ドアロック装置通信インターフェース 2 0 6 を通じて送られてきたドアロック制御モードの指示情報を受信したドアロック制御装置 1 0 0 の動作について、図 2 0 のフローチャートを参照して説明する。

15 先ず、ドアロック制御装置 1 0 0 の CPU 1 0 1 は、ドアロック制御モードの設定指示情報を監視制御装置 3 から受け取ったか否か判別し（ステップ S 6 1）、受け取らないときには、その他の処理を行なう（ステップ S 6 2）。

20 ステップ S 6 1 で、ドアロック制御モードの設定指示情報を監視制御装置 3 から受け取ったと判別したときには、CPU 1 0 1 は、選択指示されたドアロック制御モードは、オートロックモードと逐次ロックモードのいずれであるか判別する（ステップ S 6 3）。

ステップ S 6 3 で、選択指示されたドアロック制御モードはオートロックモードであると判別したときには、CPU 1 0 1 は、ドアロック装置 2 のドアロック制御モードをオートロックモードに設定する処理を行なう（ステップ S 6 4）。

25 すなわち、ステップ S 6 4 においては、ドアロック制御装置 1 0 0 の CPU 1 0 1 は、オートロックモードの設定指示に基づき、ドアロック

装置 2 の内側電子鍵リード／ライト部 2 1 i n と、外側電子鍵リード／ライト部 2 1 e x との両方をアクティブにし、かつ、プログラム R O M 1 3 のドアロック制御のアプリケーションを、オートロックモード用のものとするようにする。そして、C P U 1 0 1 は、ドアロック制御装置 1 0 0 が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、

5 1 0 0 が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、オートロックモードであることを示す情報を記憶する。

また、ステップ S 6 3 で、選択指示されたドアロック制御モードは逐次ロックモードであると判別したときには、C P U 1 0 1 は、ドアロック装置 2 のドアロック制御モードを逐次ロックモードに設定する処理を行なう（ステップ S 6 5 ）。

10 行なう（ステップ S 6 5 ）。

すなわち、ステップ S 6 5 においては、ドアロック制御装置 1 0 0 の C P U 1 0 1 は、逐次ロックモードの設定指示に基づき、この例では、ドアロック装置 2 の内側電子鍵リード／ライト部 2 1 i n と、外側電子鍵リード／ライト部 2 1 e x との両方をアクティブにし、かつ、プログラム R O M 1 3 のドアロック制御のアプリケーションを、逐次ロックモード用のものとするようにする。そして、C P U 1 0 1 は、ドアロック制御装置 1 0 0 が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶する。

15 ラム R O M 1 3 のドアロック制御のアプリケーションを、逐次ロックモード用のものとするようにする。そして、C P U 1 0 1 は、ドアロック制御装置 1 0 0 が備える不揮発性メモリ部のドアロック制御モードの記憶領域に、逐次ロックモードであることを示す情報を記憶する。

なお、この例では、逐次ロックモードにおいても、内側電子鍵リード／ライト部 2 1 i n と、外側電子鍵リード／ライト部 2 1 e x との両方を用いるようにしたが、この逐次ロックモードにおいては、外側電子鍵リード／ライト部 e x のみをアクティブにして、内側電子鍵リード／ライト部 2 1 i n を用いないようにすることもできる。その場合には、家の内側からの施錠が問題になるが、例えば、内側からの玄関ドアの施錠を、電子鍵装置を用いずにマニュアル操作で行なえる構成とすればよい。

20 /ライト部 2 1 i n と、外側電子鍵リード／ライト部 2 1 e x との両方を用いるようにしたが、この逐次ロックモードにおいては、外側電子鍵リード／ライト部 e x のみをアクティブにして、内側電子鍵リード／ライト部 2 1 i n を用いないようにすることもできる。その場合には、家の内側からの施錠が問題になるが、例えば、内側からの玄関ドアの施錠を、電子鍵装置を用いずにマニュアル操作で行なえる構成とすればよい。

25 を、電子鍵装置を用いずにマニュアル操作で行なえる構成とすればよい。

次に、オートロックモードと、逐次ロックモードのそれぞれの場合の

ドアロック装置 2 の動作について説明する。以下に説明するフローチャートにおける各ステップ S の動作は、ドアロック制御装置 100 の CPU 101 が主として実行する処理動作である。

[オートロックモード；図 21～図 26]

5 オートロックモードのときの動作を、図 21～図 26 のフローチャートを参照しながら説明する。このオートロックモードのときには、玄関ドア 1 は、定常状態では、施錠状態とされる。そして、電子鍵装置 40 が、内側電子鍵リード／ライト部 21 in または外側電子鍵リード／ライト部 21 ex にかざされて通信が両者の間で行なわれ、識別情報、す
10 なわち、電子鍵情報についての認証がとれたときには、所定時間のみ玄関ドアを開錠し、所定時間後に、自動的に玄関ドア 1 は施錠状態に戻るように、ドアロック制御装置 100 により制御されるものである。

 CPU 101 は、インターフェース 105, 106 を介して、内側電子鍵リード／ライト部 21 in および外側電子鍵リード／ライト部 21
15 ex を監視し、電子鍵装置 40 がかざされて、電子鍵装置 40 と内側電子鍵リード／ライト部 21 in または外側電子鍵リード／ライト部 21 ex との間で通信が行われるのを待つ（ステップ S 71）。

 そして、ステップ S 71 において、IC カード 40 F がかざされて、リード／ライト部 21 in または 21 ex と通信が行なわれたと判別し
20 たときには、CPU 101 は、識別情報を IC カード 40 F から受信し、例えば RAM 104 などに一時的に格納する（ステップ S 72）。このとき、ドアロック制御装置 100 が備える時計回路 122 の時刻情報も、通信があった時刻として、前記識別情報と共に RAM 104 に格納されると共に、当該時刻情報が、IC カード 40 F に与えられ、制御用 IC
25 内 42 のメモリに書き込まれる。

 また、内側電子鍵リード／ライト部 21 in または外側電子鍵リード

／ライト部 2 1 e x のどちらと通信をしたかの情報として、通信相手の I D 等が制御用 I C 4 2 のメモリに書き込まれる。

次に、C P U 1 0 1 は、内側電子鍵リード／ライト部 2 1 i n または外側電子鍵リード／ライト部 2 1 e x のどちらで I C カード 4 0 F と通信が行われたかを判別する（ステップ S 7 3）。その判別結果と、前記の通信の時刻情報とは、家族情報メモリ 1 2 0 の、前記識別情報に対応する家人の記録エリアにも、通信履歴情報として書き込まれる。また、これらの識別情報、通信時刻、内側電子鍵リード／ライト部 2 1 i n または外側電子鍵リード／ライト部 2 1 e x のどちらで I C カード 4 0 F と通信が行われたかの判別結果は、監視制御装置 3 にも、その家族情報メモリ 2 0 5 に記憶させるために転送される。

[内側電子鍵リード／ライト部 2 1 i n での通信の場合；図 2 1 ～図 2 3]

ステップ S 7 3 で、I C カード 4 0 F と通信が行われたのが内側電子鍵リード／ライト部 2 1 i n であると判別したときには、C P U 1 0 1 は、在宅者が外出する場合であるとして、以下のような処理を行なう。なお、この例では、在宅者が玄関ドア 1 を開錠し、玄関ドア 1 を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしている。

C P U 1 0 1 は、先ず、家族情報メモリ 1 2 0 に記憶されている識別情報と、I C カード 4 0 F から受信した識別情報とを比較して、家族情報メモリ 1 2 0 に記憶されている電子鍵情報としての識別情報の中に、I C カード 4 0 F から受信した識別情報と一致するものがあるかどうかにより、当該 I C カード 4 0 F がドアロック装置 2 に登録された電子鍵装置であるか否かを判別して、当該 I C カード 4 0 F についての認証を行なう（ステップ S 7 4）。

そして、その認証結果を判別し（ステップS 7 5）、家族情報メモリ 1 2 0 に記憶されている識別情報の中に、I Cカード4 0 Fから受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証N G）であると判別したときには、C P U 1 0 1 は、内側L E D駆動部 1 0 7 を駆動して、内側L E D 2 2 i nを赤色で点滅させると共に、内側スピーカ 2 3 i nから警告音を放音して、認証N GであることをI Cカード4 0 Fの使用者に報知する（ステップS 7 6）。そして、ドアロック機構 2 8 は施錠状態のままとして、ステップS 7 1に戻る。

また、ステップS 7 5で、家族情報メモリ 1 2 0 に記憶されている識別情報の中に、I Cカード4 0 Fから受信した識別情報と一致するものがあって、認証がO Kであると判別したときには、C P U 1 0 1 は、内側L E D駆動部 1 0 7 を駆動して、内側L E D 2 2 i nを緑色で1秒間点灯させ、認証O KであることをI Cカード4 0 Fの使用者に報知する（ステップS 7 7）。このとき、C P U 1 0 1により、併せて内側スピーカ 2 3 i nから「認証がとれました」というメッセージを放音させるようにしても良い。

そして、このとき、認証がO Kであることから、C P U 1 0 1 は、ドアロック機構駆動部 1 1 2 を駆動制御して、ドアロック機構 2 8 により玄関ドア 1 を開錠状態にし（ステップS 7 8）、内側スピーカ 2 3 i n から、「ドアロックを解除しました」というメッセージを放音させる（ステップS 7 9）。このとき、内側L E D 2 2 i nを、例えば緑色で点滅させ、ドアロックの解除状態をI Cカード4 0 Fの使用者に報知するようにしてもよい。

このとき、C P U 1 0 1 は、I Cカード4 0 Fにより内側から玄関ドア 1 が開錠されたことを認識していることに基づき、当該I Cカード4 0 Fの使用者（在宅者）が外出しようとしていると認識する。そして、

監視制御装置 3 に対して窓の開閉状態についての問い合わせを送る（図 22 のステップ S 8 1）。

これに対して、監視制御装置 3 では、窓センサ 6 a , 6 b のセンサ出力をセンサハブ 2 0 7 を通じて取得して、窓の開閉を確認する。つまり、
5 戸締りを確認する。そして、窓の開閉状態についての確認結果をドアロック装置インターフェース 2 0 6 を通じてドアロック制御装置 1 0 0 に返信するようにする。

ドアロック制御装置 1 0 0 では、この窓の開閉状態についての確認結果を、通信インターフェース 1 2 1 を通じて受信する（ステップ S 8 2）。
10 そして、CPU 1 0 1 は、受信した当該確認結果を解析して、窓が開放されているか否か判別する（ステップ S 8 3）。

そして、窓が開いていると判別したときには、CPU 1 0 1 は、窓が開いていることを内側スピーカ 2 3 i n からの放音音声により警告する（ステップ S 8 4）。また、窓が閉じていると判別したときには、CPU
15 U 1 0 1 は、戸締りが OK であることを内側スピーカ 2 3 i n からの放音音声により報知する（ステップ S 8 5）。

次に、CPU 1 0 1 は、ドア開閉センサ 2 7 のセンサ出力をインターフェース 1 1 1 を通じて取り込み、玄関ドア 1 が開けられた否か監視する（ステップ S 8 6）。そして、CPU 1 0 1 は、玄関ドア 1 が開けられ
20 ずに所定時間、例えば 1 0 秒経過したかどうかを判別し（ステップ S 8 7）、1 0 秒経過したと判別したときには、玄関ドア 1 を自動的に施錠状態に戻すようにする（ステップ S 8 8）。そして、CPU 1 0 1 は、内側 LED 2 2 i n を緑色で点滅して、玄関ドア 1 が施錠状態に戻ったことを報知する（ステップ S 8 9）。

25 また、ステップ S 8 6 で、ステップ S 7 8 での開錠後、1 0 秒以内に玄関ドア 1 が開かれたと判別したときには、CPU 1 0 1 は、ステップ

S 7 2 で取り込んだ識別情報で示される在宅者が外出をしたと認識して、当該識別情報、時刻情報を含む個人情報、外出者情報として監視制御装置 3 に転送する（ステップ S 9 0）。なお、このとき監視制御装置 3 に転送する情報には時刻情報を含めず、監視制御装置 3 がこれらの情報を受信した時刻を、時計回路 2 2 1 の時刻から認識するようにすることもできる。

その後、CPU 1 0 1 は、ドア開閉センサ 2 7 のセンサ出力を参照して、玄関ドア 1 が閉じられたことを確認し（ステップ S 9 1）、玄関ドア 1 が閉じられた後、所定時間、例えば 3 秒経過したことを確認したら（ステップ S 9 2）、ドアロック機構駆動部 1 1 2 を駆動制御して、ドアロック機構 2 8 により玄関ドア 1 を施錠状態に復帰させるようにする（図 2 3 のステップ S 1 0 1）。そして、CPU 1 0 1 は、外側 LED 2 2 e x を緑色で点滅して、玄関ドア 1 が施錠状態に戻ったことを IC カード 4 0 F の使用者に報知する（ステップ S 1 0 2）。この外側 LED 2 2 e x の緑色点滅は、所定時間、例えば 1 0 秒間続けられる。

その後、CPU 1 0 1 は、前記所定時間、例えば 1 0 秒経過したか否か判別し（ステップ S 1 0 3）、所定時間経過していないと判別したときには、ステップ S 7 1 で通信が行われたと判別された IC カード 4 0 F が、再度、外側電子鍵リード／ライト部 2 1 e x と通信したか否か判別する（ステップ S 1 0 4）、通信がなされないと判別したときにはステップ S 1 0 3 に戻る。

そして、ステップ S 1 0 3 で、IC カード 4 0 F と外側電子鍵リード／ライト部 2 1 e x とで通信が行われずに、前記所定時間経過したと判別したときには、CPU 1 0 1 は、内側電子鍵リード／ライト部 2 1 i n に対して IC カード 4 0 F がかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図 2 1 のステップ S 7 1 に戻

る。

また、ステップS 1 0 4で、玄関ドア施錠復帰後、外側LED 2 2 e xの緑色点滅が終了する所定時間経過する前に、ステップS 7 1において通信が行われたと判別されたICカード4 0 Fと外側電子鍵リード／
5 ライト部2 1 e xとで通信が行われたと判別すると、ステップS 1 0 1～S 6 3で確認された戸締りを再確認する（ステップS 1 0 5）。

ステップS 1 0 5で、戸締りがOKであると判別したときには、CPU 1 0 1は、通信インターフェース1 2 1を通じてセキュリティモードをオンにする要求を監視制御装置3に送信する（ステップS 1 0 6）。

- 10 この要求に対しては、監視制御装置3は、そのときの在宅状況をチェックして、セキュリティレベルが図1 5に示したいずれのレベルとなるかを判定する。そして、監視制御装置3は、その判定の結果、セキュリティレベルがレベルDであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置1 0 0に返し、セキュリティ
15 レベルがレベルD以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置1 0 0に返す。

- ドアロック制御装置1 0 0のCPU 1 0 1は、監視制御装置3からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップS 1 0 7）。そして、
20 セキュリティモードがオンにできる旨の返答を監視制御装置3から受けたと判別したときには、CPU 1 0 1は、外側スピーカ2 3 e xから、「セキュリティモードをオンにします」というメッセージを放音させる（ステップS 1 0 8）。

【0 1 9 8】

- 25 また、ステップS 1 0 7で、セキュリティモードがオンにできない旨の返答を監視制御装置3から受けたと判別したときには、CPU 1 0 1

は、外側スピーカ 2 3 e x から、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップ S 1 0 9）。その後、ステップ S 7 1 に戻る。

5 また、ステップ S 1 0 5 で、窓が開いていて戸締りが完了していないと判別したときには、CPU 1 0 1 は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップ S 1 1 0）。そして、その後、ステップ S 7 1 に戻る。

10 [外側電子鍵リード／ライト部 2 1 e x での通信の場合；図 2 4 ～図 2 6]

ステップ S 7 1 で、IC カード 4 0 F と通信が行われたのが外側電子鍵リード／ライト部 2 1 e x であると判別したときには、CPU 1 0 1 は、家人が帰宅した場合あるいはその他の外にいる者の入室要求であるとして、以下のような処理を行なう。

15 CPU 1 0 1 は、まず、家族情報メモリ 1 2 0 に記憶されている識別情報と、IC カード 4 0 F から受信した識別情報とを比較して、家族情報メモリ 1 2 0 に記憶されている識別情報の中に、IC カード 4 0 F から受信した識別情報と一致するものがあるかどうかにより、当該 IC カード 4 0 F がドアロック装置 2 に登録された IC カード 4 0 F であるか
20 否かを判別して、当該 IC カード 4 0 F についての認証を行なう（ステップ S 1 2 1）。

そして、その認証結果を判別し（ステップ S 1 2 2）、家族情報メモリ 1 2 0 に記憶されている識別情報の中に、IC カード 4 0 F から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証
25 NG）であると判別したときには、CPU 1 0 1 は、外側 LED 駆動部 1 0 8 を駆動して、外側 LED 2 2 e x を赤色で点滅させると共に、外

側スピーカ 23 e x から警告音を放音して、認証 N G であることを I C
カード 40 F の使用者に報知する（ステップ S 1 2 3）。そして、ドア
ロック機構 28 は施錠状態のままとして、ステップ S 7 1 に戻る。

また、ステップ S 1 2 2 で、家族情報メモリ 120 に記憶されている
5 識別情報の中に、I C カード 40 F から受信した識別情報と一致するも
のがあって、認証が O K であると判別したときには、C P U 101 は、
外側 L E D 駆動部 108 を駆動して、外側 L E D 22 e x を緑色で1秒
間点灯させ、認証 O K であることを I C カード 40 F の使用者に報知す
る（ステップ S 1 2 4）。このとき、C P U 101 により、合わせて外
10 側スピーカ 23 e x から「認証がとれました」というメッセージを放音
させるようにしても良い。

そして、このとき、認証が O K であることから、C P U 101 は、ド
アロック機構駆動部 112 を駆動制御して、ドアロック機構 28 により
玄関ドア 1 を開錠状態にし（ステップ S 1 2 5）、外側スピーカ 23 e
15 x から、「ドアロックを解除しました」というメッセージを放音させる
（ステップ S 1 2 6）。このとき、外側 L E D 22 e x を、例えば緑色
で点滅させ、ドアロックの解除状態を I C カード 40 F の使用者に報知
するようにしてもよい。

次に、C P U 101 は、ドア開閉センサ 27 のセンサ出力をインター
20 フェース 111 を通じて取り込み、玄関ドア 1 が開けられた否か監視す
る（ステップ S 1 2 7）。そして、C P U 101 は、玄関ドア 1 が開け
られずに所定時間、例えば10秒経過したかどうかを判別し（ステップ
S 1 2 8）、10秒経過したと判別したときには、玄関ドア 1 を自動的
に施錠状態に戻すようにする（ステップ S 1 2 9）。そして、C P U 1
25 01 は、外側 L E D 22 e x を緑色で点滅して、玄関ドア 1 が施錠状態
に戻ったことを報知する（ステップ S 1 3 0）。

その後、CPU101は、所定時間、例えば10秒経過したか否か判別し（ステップS131）、所定時間経過していないと判別したときには、ステップS71で通信が行われたと判別された電子鍵装置が外側電子鍵リード／ライト部21exと通信したか否か判別し（ステップS132）、通信がなされないと判別したときにはステップS131に戻る。

そして、ステップS131で、電子鍵装置と外側電子鍵リード／ライト部21exとで通信が行われずに、所定時間経過したと判別したときには、CPU101は、外側電子鍵リード／ライト部21exに対して電子鍵装置がかざされたことにより開始された玄関ドアのロック制御動作が一段落したとして、図21のステップS71に戻る。

また、ステップS132で、玄関ドア施錠復帰後、所定時間経過する前に、ステップS71において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部21exとで通信が行われたと判別すると、戸締りを確認する（ステップS133）。

このステップS133での戸締りの確認は、前述のステップS121～S123において説明した処理と同様に行なう。つまり、ドアロック制御装置100は、監視制御装置3に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置3から取得する。そして、その問い合わせ結果から、戸締りがOKかどうかを判別する。

ステップS133で、戸締りがOKであると判別したときには、CPU101は、通信インターフェース121を通じてセキュリティモードをオンにする要求を監視制御装置3に送信する（ステップS134）。

この要求に対しては、監視制御装置3は、そのときの在宅状況をチェックして、セキュリティレベルが図15に示したいずれのレベルとなるかを判定する。そして、監視制御装置3は、その判定の結果、セキュリティレベルがレベルDであるときには、セキュリティモードはオンにで

きないので、その旨をドアロック制御装置 100 に返し、セキュリティレベルがレベル D 以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置 100 に返す。

5 ドアロック制御装置 100 の CPU 101 は、監視制御装置 3 からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップ S 135）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置 3 から受けたと判別したときには、CPU 101 は、外側スピーカ 23 ex から、
10 「セキュリティモードをオンにします」というメッセージを放音させる（ステップ S 136）。

また、ステップ S 135 で、セキュリティモードがオンにできない旨の返答を監視制御装置 3 から受けたと判別したときには、CPU 101 は、外側スピーカ 23 ex から、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステップ S 137）。その後、ステップ S 71 に戻る。
15

また、ステップ S 133 で、窓が開いていて戸締りが完了していないと判別したときには、CPU 101 は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを放音する（ステップ S 138）。そして、その後、ステップ S 71 に戻る。
20

ステップ S 131 ～ステップ S 138 の処理は、一旦、玄関ドア 1 を内側から開錠した後、所定時間以内に、外側電子鍵リード／ライト部 21 ex に電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた者が、もう一度、室内に戻って、内側電子鍵リード／ライト部 21 in に対して電子鍵装置をかざすところからやり直す手間を防止するための処理である。
25

すなわち、一旦、玄関ドア 1 を内側から開錠した後、所定時間以内に、外側電子鍵リード／ライト部 2 1 e x に電子鍵装置をかざして、セキュリティモードをオンにするのを忘れた、あるいは失敗した場合に、外側電子鍵リード／ライト部 2 1 e x に電子鍵装置をかざして、玄関ドア 1
5 を一旦開錠させ、その後、10 秒待つて再施錠になった後、10 秒以内に、再び、外側電子鍵リード／ライト部 2 1 e x に電子鍵装置をかざすことにより、セキュリティモードをオンにすることができるものである。このようにすれば、セキュリティモードをオンに設定するために、開錠してから室内に入り、内側電子鍵リード／ライト部 2 1 i n に電子鍵装
10 置 4 0 をかざすところからやり直す必要がなく、便利である。

次に、ステップ S 1 2 7 で、ステップ S 1 2 5 での開錠後、10 秒以内に玄関ドア 1 が開かれたと判別したときには、CPU 1 0 1 は、ステップ S 7 2 で取り込んだ識別情報で示される外出者が帰宅したと認識して、当該識別情報、電子鍵装置と通信が行なわれた時刻情報を含む個人
15 情報を、帰宅者情報として監視制御装置 3 に転送する（図 2 6 のステップ S 1 4 1）。なお、このとき監視制御装置 3 に転送する情報には時刻情報を含めず、監視制御装置 3 がこれらの情報を受信した時刻を、時計回路 2 2 1 の時刻から認識するようにすることもできる。

その後、CPU 1 0 1 は、ドア開閉センサ 2 7 のセンサ出力を参照して、玄関ドア 1 が閉じられたことを確認し（ステップ S 1 4 2）、玄関
20 ドア 1 が閉じられた後、所定時間、例えば 3 秒経過したことを確認したら（ステップ S 1 4 3）、ドアロック機構駆動部 1 1 2 を駆動制御して、ドアロック機構 2 8 により玄関ドア 1 を施錠状態に復帰させるようにする（ステップ S 1 4 4）。そして、CPU 1 0 1 は、内側 LED 2 2 i
25 n を緑色で点滅して、玄関ドア 1 が施錠状態に戻ったことを報知する（ステップ S 1 4 5）。

その後、CPU 101は、帰宅者があったことから在宅状況が変更することに基つき、セキュリティレベルの変更指示を監視制御装置3に送る（ステップS146）。

このセキュリティレベルの変更指示を受け取った監視制御装置3では、
5 ステップS141での帰宅者情報による在宅状況の変化を認識し、図15に示した在宅状況とセキュリティレベルとの対応テーブルを参照して、セキュリティレベルの変更の必要があるか否かを判別し、必要があるときには、セキュリティレベルを変更する。そして、監視制御装置3は、セキュリティレベルを変更したかどうかを、ドアロック制御装置100に
10 通知する。

ドアロック制御装置100のCPU101は、監視制御装置3からのセキュリティレベルの変更に関する通知を受け取って（ステップS147）、セキュリティレベルが変更されたか否かを判別する（ステップS148）。

そして、ステップS148で、セキュリティモードが変更されたと判別したときには、CPU101は、内側スピーカ23inから、「セキュリティレベルを変更しました」というメッセージを放音する（ステップS149）。そして、ステップS71に戻る。

なお、以上の説明では、帰宅者があったときには、ドアロック制御装置100から、ステップS146において、監視制御装置3にセキュリティレベルの変更指示を送るようにしたが、監視制御装置3では、ステップS141での帰宅者情報の転送を受けるので、ドアロック制御装置100からのセキュリティレベルの変更指示を受けなくても、自動的にセキュリティレベルの変更が必要かどうかを判断して、必要である場合には、セキュリティレベルを自動的に変更するようにしても良い。その
20 場合には、セキュリティレベルを変更したときには、その旨をドアロッ
25

ク制御装置 100 に転送するようにする。

[逐次ロックモードの説明；図 27～図 29]

次に、逐次ロックモードのときの動作を、図 27～図 29 のフローチャートを参照しながら説明する。この逐次ロックモードのときには、IC カード 40C が、内側電子鍵リード／ライト部 21in または外側電子鍵リード／ライト部 21ex にかざされて通信が両者の間で行なわれ、電子鍵情報としての識別情報についての認証がとれたときには、そのときの玄関ドア 1 の開錠あるいは施錠の状態とは逆の状態になるように、ドアロック機構 28 は、ドアロック制御装置 100 により制御されるものである。

CPU 101 は、インターフェース 105, 106 を介して、内側電子鍵リード／ライト部 21in および外側電子鍵リード／ライト部 21ex を監視し、IC カード 40C がかざされて、IC カード 40C と内側電子鍵リード／ライト部 21in または外側電子鍵リード／ライト部 21ex との間で通信が行われるのを待つ（ステップ S151）。

そして、ステップ S151 において、IC カード 40F がかざされて、IC カード 40F と通信が行なわれたと判別したときには、CPU 101 は、識別情報を IC カード 40F から受信し、例えば RAM 104 などに一時的に格納する（ステップ S152）。このとき、前述と同様に、IC カード 40F には時刻情報等が書き込まれると共に、家族情報メモリ 120 および監視制御装置 3 の家族情報メモリ 205 への時刻情報等の書き込みが行なわれる。

内側電子鍵リード／ライト部 21in または外側電子鍵リード／ライト部 21ex のどちらで IC カード 40F と通信が行われたかを判別する（ステップ S153）。

[内側電子鍵リード／ライト部 21in での通信の場合；図 27]

ステップS 1 5 3で、I Cカード4 0 Fと通信が行われたのが内側電子鍵リード／ライト部2 1 i nであると判別したときには、C P U 1 0 1は、在宅者が外出する場合あるいは玄関ドア1をセキュリティのために施錠する場合であるとして、以下のような処理を行なう。

5 C P U 1 0 1は、先ず、家族情報メモリ1 2 0に記憶されている識別情報と、I Cカード4 0 Fから受信した識別情報とを比較して、家族情報メモリ1 2 0に記憶されている識別情報の中に、I Cカード4 0 Fから受信した識別情報と一致するものがあるかどうかにより、当該I Cカード4 0 Fがドアロック装置2に登録された電子鍵装置であるか否かを
10 判別して、当該I Cカード4 0 Fについての認証を行なう（ステップS 1 5 4）。

そして、その認証結果を判別し（ステップS 1 5 5）、家族情報メモリ1 2 0に記憶されている識別情報の中に、I Cカード4 0 Fから受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証
15 N G）であると判別したときには、C P U 1 0 1は、内側L E D駆動部1 0 7を駆動して、内側L E D 2 2 i nを赤色で点滅させると共に、内側スピーカ2 3 i nから警告音を放音して、認証N GであることをI Cカード4 0 Fの使用者に報知する（ステップS 1 5 6）。そして、ドアロック機構2 8は、その前の状態のままとして、ステップS 1 5 1に戻る。
20

また、ステップS 1 5 5で、家族情報メモリ1 2 0に記憶されている識別情報の中に、I Cカード4 0 Fから受信した識別情報と一致するものがあって、認証がO Kであると判別したときには、C P U 1 0 1は、内側L E D駆動部1 0 7を駆動して、内側L E D 2 2 i nを緑色で1秒
25 間点灯させ、認証O KであることをI Cカード4 0 Fの使用者に報知する（ステップS 1 5 7）。このとき、C P U 1 0 1により、併せて内側

スピーカ 23 in から「認証がとれました」というメッセージを放音させるようにしても良い。

そして、CPU 101 は、現在のドアロック機構 28 による玄関ドア 1 のロック状態は、施錠状態になっているか否か判別する（ステップ S 158）。このステップ S 158 で、ドアロック機構 28 による玄関ドア 1 のロック状態が、開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部 112 を駆動制御する（ステップ S 159）。

そして、CPU 101 は、内側 LED 22 in を、例えば緑色で点滅させると共に、内側スピーカ 23 in から、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことを IC カード 40 F の使用者に報知するようにする（ステップ S 160）。

そして、CPU 101 は、ステップ S 152 で取り込んだ識別情報で示される者が、セキュリティのために施錠をしたと認識して、当該識別情報を含む個人情報を、在宅者情報として監視制御装置 3 に転送する（ステップ S 161）。

また、ステップ S 158 で、現在のドアロック機構 28 のロック状態は、施錠状態であると判別したときには、CPU 101 は、ドアロック機構駆動部 112 を駆動制御して、ドアロック機構 28 を開錠状態にし（ステップ S 162）、内側 LED 22 in を、例えば緑色で点滅させると共に、内側スピーカ 23 in から、「ドアロックを解除しました」というメッセージを放音させる（ステップ S 163）。

そして、このときには、CPU 101 は、ステップ S 152 で取り込んだ識別情報で示される者が、開錠をして外出をしたと認識して、当該識別情報を含む個人情報を、外出者情報として監視制御装置 3 に転送する（ステップ S 164）。

[外側電子鍵リード／ライト部 2 1 e x での通信の場合；図 2 8 ～図 2 9]

ステップ S 1 5 3 で、I C カード 4 0 F と通信が行われたのが外側電子鍵リード／ライト部 2 1 e x であると判別したときには、C P U 1 0 1 は、家人が帰宅して開錠する場合あるいは家人が外出のため施錠する場合であるとして、以下のような処理を行なう。

C P U 1 0 1 は、まず、家族情報メモリ 1 2 0 に記憶されている識別情報と、I C カード 4 0 F から受信した識別情報とを比較して、家族情報メモリ 1 2 0 に記憶されている識別情報の中に、I C カード 4 0 F から受信した識別情報と一致するものがあるかどうかにより、当該 I C カード 4 0 F がドアロック装置 2 に登録された電子鍵装置であるか否かを判別して、当該 I C カード 4 0 F についての認証を行なう（ステップ S 1 7 1）。

そして、その認証結果を判別し（ステップ S 1 7 2）、家族情報メモリ 1 2 0 に記憶されている識別情報の中に、I C カード 4 0 F から受信した識別情報と一致するものがなくて、認証が取れなかったとき（認証 N G）であると判別したときには、C P U 1 0 1 は、外側 L E D 駆動部 1 0 8 を駆動して、外側 L E D 2 2 e x を赤色で点滅させると共に、外側スピーカ 2 3 e x から警告音を放音して、認証 N G であることを I C カード 4 0 F の使用者に報知する（ステップ S 1 7 3）。そして、ドアロック機構 2 8 は施錠状態のままとして、ステップ S 1 5 1 に戻る。

また、ステップ S 1 7 2 で、家族情報メモリ 1 2 0 に記憶されている識別情報の中に、I C カード 4 0 F から受信した識別情報と一致するものがあって、認証が O K であると判別したときには、C P U 1 0 1 は、外側 L E D 駆動部 1 0 8 を駆動して、外側 L E D 2 2 e x を緑色で 1 秒間点灯させ、認証 O K であることを I C カード 4 0 F の使用者に報知す

る（ステップS 1 7 4）。このとき、CPU 1 0 1により、併せて外側スピーカ 2 3 e xから「認証がとれました」というメッセージを放音させるようにしても良い。

そして、CPU 1 0 1は、現在のドアロック機構 2 8のロック状態は、
5 施錠状態になっているか否か判別する（ステップS 1 7 5）。このステップS 1 7 5で、現在のドアロック機構 2 8による玄関ドア 1のロック状態は、施錠状態であると判別したときには、CPU 1 0 1は、ドアロック機構駆動部 1 1 2を駆動制御して、ドアロック機構 2 8により玄関
10 ドア 1を開錠状態にし（ステップS 1 7 6）、内側LED 2 2 i nを、例えば緑色で点滅させると共に、内側スピーカ 2 3 i nから、「ドアロックを解除しました」というメッセージを放音させる（ステップS 1 7 7）。

そして、CPU 1 0 1は、ステップS 1 5 2で取り込んだ識別情報で示される者が、帰宅のため開錠をしたと認識して、当該識別情報および
15 帰宅時刻情報（電子鍵装置と通信が行なわれた時刻）を含む個人情報を、帰宅者情報として監視制御装置 3に転送する（ステップS 1 7 8）。この場合にも、前述と同様にして、監視制御装置 3がこれらの情報を受信した時刻を、時計回路 2 2 1の時刻から認識して、その時刻を帰宅時刻とするようにしてもよい。

20 また、ステップS 1 7 5で、現在の玄関ドア 1のロック状態が開錠状態であると判別したときには、その逆の状態である施錠状態にするように、ドアロック機構駆動部 1 1 2を駆動制御して、ドアロック機構 2 8により玄関ドア 1を施錠状態にする（ステップS 1 7 9）。

そして、CPU 1 0 1は、内側LED 2 2 i nを、例えば緑色で点滅
25 させると共に、内側スピーカ 2 3 i nから、「玄関ドアを施錠しました」というメッセージを放音させ、施錠状態にしたことをICカード 4 0 F

の使用者に報知するようにする（ステップS180）。

そして、CPU101は、ステップS152で取り込んだ識別情報で示される者が、外出のために施錠をしたと認識して、当該識別情報を含む個人情報、外出者情報として監視制御装置3に転送する（ステップS181）。

そして、施錠後、CPU101は、所定時間、例えば10秒経過したか否か判別し（図29のステップS182）、所定時間経過していないと判別したときには、ステップS171で通信が行われたと判別されたICカード40Fが、再度、外側電子鍵リード／ライト部21exと通信したか否か判別し（ステップS183）、通信がなされないと判別したときにはステップS182に戻る。

また、ステップS183で、玄関ドア施錠後、所定時間経過する前に、ステップS71において通信が行われたと判別された電子鍵装置と外側電子鍵リード／ライト部21exとで通信が行われたと判別すると、戸締りを確認する（ステップS184）。

このステップS184での戸締りの確認は、前述のステップS101～S103において説明した処理と同様に行なう。つまり、ドアロック制御装置100は、監視制御装置3に対して窓の開閉状態についての問い合わせを行ない、問い合わせ結果を監視制御装置3から取得する。そして、その問い合わせ結果から、戸締りがOKかどうかを判別する。

ステップS184で、戸締りがOKであると判別したときには、CPU101は、通信インターフェース121を通じてセキュリティモードをオンにする要求を監視制御装置3に送信する（ステップS185）。

この要求に対しては、監視制御装置3は、そのときの在宅状況をチェックして、セキュリティレベルが図15に示したいずれのレベルとなるかを判定する。そして、監視制御装置3は、その判定の結果、セキュリ

ティレベルがレベルDであるときには、セキュリティモードはオンにできないので、その旨をドアロック制御装置100に返し、セキュリティレベルがレベルD以外であるときには、セキュリティモードをオンにできるので、その旨をドアロック制御装置100に返す。

- 5 ドアロック制御装置100のCPU101は、監視制御装置3からのセキュリティモードオンの要求に対する返答を解析して、セキュリティモードをオンにできるか否か判別する（ステップS186）。そして、セキュリティモードがオンにできる旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、
- 10 「セキュリティモードをオンにします」というメッセージを放音させる（ステップS187）。

- また、ステップS186で、セキュリティモードがオンにできない旨の返答を監視制御装置3から受けたと判別したときには、CPU101は、外側スピーカ23exから、「在宅者が存在するため、セキュリティモードをオンにはできません」というメッセージを放音させる（ステ
- 15 ップS188）。その後、ステップS151に戻る。

- また、ステップS184で、窓が開いていて戸締りが完了していないと判別したときには、CPU101は、「窓が開いているため、セキュリティモードをオンにすることはできません」という警告メッセージを
- 20 放音する（ステップS189）。そして、その後、ステップS171に戻る。

[監視制御装置3におけるセキュリティ動作；図30]

- 上述のようにして、監視制御装置3は、ドアロック制御装置100からの指示を受けてセキュリティモードをオンにするが、リモートコマン
- 25 ダ50のセキュリティボタン51を押すことによってもセキュリティモードをオンにすることができる。そして、監視制御装置3のセキュリテ

ィモードオン状態は、リモートコマンド 50 のオフボタン 52 を操作すると、オフとすることができる。

図 30 は、リモートコマンド 50 を操作することにより、監視制御装置 3 のセキュリティモードのオン・オフを制御する動作を説明するための
5 のフローチャートである。

まず、CPU 201 は、リモートコマンド 50 からの遠隔操作信号を監視して、リモートコマンド 50 で操作入力となされたか否か判別する（ステップ S 191）。そして、操作入力となされたと判別したときには、CPU 201 は、操作されたのはセキュリティボタン 51 であるか
10 否か判別する（ステップ S 192）。

ステップ S 192 での判別の結果、セキュリティボタン 51 の操作であると判別したときには、CPU 201 は、リモコン送信部 39 から電源オンのリモコン信号をテレビ受像機 7 のリモコン受信部に送り、テレビ受像機 7 をオンにする（ステップ S 193）。

そして、CPU 201 は、ROM 203 から読み出したデータに基づいて生成した画像情報を、テレビインターフェース 217 を通じてテレビ受像機 7 に送り、テレビ受像機 7 の画面にセキュリティモードオンの確認画面を表示する（ステップ S 194）。その後、CPU 201 は、リモコン送信部 39 からテレビ受像機 7 の電源をオフするリモコン信号
20 を送出して、テレビ受像機 7 をオフさせる（ステップ S 195）。

そして、CPU 201 は、その所定時間、例えば 5 分経過後（ステップ S 196）、セキュリティモードをオンにして（ステップ S 197）、セキュリティ監視動作を実行する（ステップ S 198）。ステップ S 196 における所定時間は、セキュリティボタン 51 を操作した使用者が、
25 セキュリティモードオンに設定した後、玄関ドアから退出するまでの時間を考慮した時間とされている。

ステップS 1 9 2において、リモートコマンド5 0で操作されたボタンがセキュリティボタン5 1ではないと判別したときには、CPU 2 0 1は、操作されたのはオフボタン5 2であるか否か判別する（ステップS 1 9 9）。このステップS 1 9 9でオフボタン5 2ではないと判別したときには、CPU 2 0 1は、その他のボタンが押されたことによる処理を実行する（ステップS 2 0 0）。

ステップS 1 9 9での判別の結果、オフボタン5 2であると判別したときには、CPU 2 0 1は、リモコン送信部3 9から電源オンのリモコン信号をテレビ受像機7のリモコン受信部に送り、テレビ受像機7をオンにする（ステップS 2 0 1）。

そして、CPU 2 0 1は、ROM 2 0 3から読み出したデータに基づいて生成した画像情報を、テレビインターフェース2 1 7を通じてテレビ受像機7に送り、テレビ受像機7の画面にセキュリティモードオフの確認画面を表示する（ステップS 2 0 2）。その後、CPU 2 0 1は、リモコン送信部3 9からテレビ受像機7の電源をオフするリモコン信号を送出して、テレビ受像機7をオフさせる（ステップS 2 0 3）。

そして、CPU 2 0 1は、セキュリティモードをオフにする処理を行なう（ステップS 2 0 4）。以上で、図3 0の処理ルーチンは終了となる。

[セキュリティモードオンにおける監視動作]

図3 1および図3 2は、監視制御装置3において、セキュリティモードオンとされたときの処理動作である。これは、前述のリモートコマンド5 0でのセキュリティボタン5 1の操作時に起動されるもので、このときのセキュリティレベルは、レベルAの場合である。なお、ドアロック制御装置1 0 0からのセキュリティモードオン指示があったときには、前述したように、在宅者の状況が参酌されてセキュリティレベルが決定

され、その決定されたセキュリティレベルでセキュリティモードがオンとされるものである。

図 3 1 においては、先ず、CPU 2 0 1 は、ビデオカメラ 3 1 の撮影画像の取り込みを開始する（ステップ S 2 1 1）。このとき、マイクロホン 3 4 で收音した音声も一緒に取り込みを行なう。前述したように、
5 画像・音声メモリ 2 0 8 に設けられるセキュリティモード用の監視情報領域は、リングバッファ形式とされており、この例では、最新の 3 0 秒分の画像・音声情報が常に画像・音声メモリ 2 0 8 に格納されるようにされている。監視カメラ 1 3 からの撮影画像についても同様にされている。
10 る。

次に、CPU 2 0 1 は、センサハブ 2 0 7 からの窓センサ 1 6 a、1 6 b のセンサ出力と、玄関ドア 1 のドア開閉センサ 2 7 のセンサ出力の監視を開始するように制御する（ステップ S 2 1 2）。さらに、CPU 2 0 1 は、火災センサ 4 およびガスセンサ 5 のセンサ出力の監視を開始
15 するように制御する（ステップ S 2 1 3）。監視カメラ 1 3 は、火災センサ 4 やガスセンサ 5 のオン・オフに応じてオン・オフする。

次に、CPU 2 0 1 は、人感センサ 3 3 のセンサ出力を監視して、侵入者がいないかどうかチェックする（ステップ S 2 1 4）。侵入者なしと判別したときには、窓センサ 1 6 a、1 6 b のセンサ出力や、ドア開閉
20 センサ 2 7 のセンサ出力から、異常を検知したか否か判別する（図 3 2 のステップ S 2 3 1）。

ステップ S 2 3 1 で、異常を検知しないと判別したときには、CPU 2 0 1 は、火災センサ 4 やガスセンサ 5 のセンサ出力から、異常を検知したか否か判別する（ステップ S 2 3 2）。ステップ S 2 3 2 で、異常
25 を検知しないと判別したときには、ステップ S 2 1 4 に戻る。

そして、ステップ S 2 1 4 で、侵入者を人感センサ 3 3 により検知し

たと判別したときには、CPU 201は、照明機構 320を制御して、照明 32をオンにする（ステップ S 215）。そして、侵入者の検知時点の 10秒前から、検知時点の 20秒後までの 30秒分の画像・音声情報を、画像・音声メモリ 208から読み出し、1回目の画像として、管理サーバ装置 10に転送する（ステップ S 216）。管理サーバ装置 10では、この転送されてきた画像・音声情報により、侵入者を認識して、適切な処置を取ることができる。

次に、CPU 201は、リモコン送信部 39からテレビ受像機 7に電源オンのリモコン信号を送り、テレビ受像機 7をオンにする（ステップ S 217）。そして、CPU 201は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機 7に送り、それら威嚇画像および威嚇音声を出力する（ステップ S 218）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

次に、CPU 201は、監視制御装置 3に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップ S 219）。

そして、CPU 201は、その後、数秒間隔で、画像・音声メモリ 208のリングバッファに格納されている 30秒分の画像・音声情報を繰り返し管理サーバ装置 10に転送する（ステップ S 220）。そして、CPU 201は、人感センサ 33が侵入者を検知しなくなったか否か判別し（ステップ S 221）、検知しなくなるまで、30秒分の画像・音声情報を管理サーバ装置 10に転送する処理作業を継続する。

そして、CPU 201は、人感センサ 33が侵入者を検知しなくなったと判別したときには、30秒分の画像・音声情報の管理サーバ装置 10への転送を中止する（ステップ S 222）。そして、ステップ S 231に戻って、セキュリティ監視を続ける。

また、ステップS 2 3 1において、異常を検知したと判別したときには、CPU 2 0 1は、窓センサ6 a, 6 bやドア開閉センサ2 7の近傍に設置されている監視カメラ1 3からの検知時点の1 0秒前から、検知時点の2 0秒後までの3 0秒分画像を1回目として、管理サーバ装置1 5 0に転送する（ステップS 2 3 4）。

そして、CPU 2 0 1は、リモコン送信部3 9からテレビ受像機7に電源オンのリモコン信号を送り、テレビ受像機7をオンにする（ステップS 2 3 5）。そして、CPU 2 0 1は、予め用意している威嚇画像および威嚇音声の情報をテレビ受像機7に送り、それら威嚇画像および威嚇音声10 を出力する（ステップS 2 3 6）。この威嚇画像・音声により侵入した賊を威嚇して、退散させることが可能となる。

次に、CPU 2 0 1は、監視制御装置3に予め登録されている連絡先、例えば警備会社、警察署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップS 2 3 7）。

そして、CPU 2 0 1は、その後、数秒間隔で、画像・音声メモリ2 15 0 8のリングバッファに格納されている3 0秒分の画像・音声情報を繰り返し管理サーバ装置1 0に転送する（ステップS 2 3 8）。そして、CPU 2 0 1は、リモートコマンド5 0のオフボタン5 2によるオフ指示を待ち（ステップS 2 3 9）、オフ指示が有ったときには、セキュリティ20 モードをオフとする。

また、ステップS 2 3 2で、火災センサ4またはガスセンサ5で異常が検知されたと判別したときには、CPU 2 0 1は、監視制御装置3に設定登録されている、例えば警備会社、消防署の他、登録された家人の携帯電話に対して異常検知を連絡する（ステップS 2 3 3）。そして、25 ステップS 2 3 9に進む。

なお、画像・音声情報を監視制御装置3から受け取った管理サーバ装

置 10 は、W e b ページにそれらの画像・音声情報を載せる。そこで、監視制御装置 3 から連絡を受け取った携帯電話の持ち主は、管理サーバ装置 10 の当該 W e b ページにアクセスして、どのような異常が発生したかを知ることができ、適切な対応処置を講じることが可能になる。

5 [監視制御装置 3 におけるドアロック制御装置 100 からの指示による連携；図 33]

監視制御装置 3 の C P U 201 は、ドアロック制御装置 100 から受け取った情報や指示に応じて、図 33 に示すような連携動作を行なう。

10 なお、この例は、セキュリティレベルの変更は、C P U 201 が、ドアロック制御装置 100 からの変更指示を受けて行なうのではなく、ドアロック制御装置 100 からの個人情報を受け取った結果による在宅状況の変化をチェックして、必要に応じて行なうようにした場合である。

すなわち、C P U 201 は、ドアロック制御装置 100 からセキュリティモードオンの指示を受け取ったか否か判別する(ステップ S 241)。

15 受け取らないと判別したときには、C P U 201 は、その他の処理を行なう(ステップ S 242)。

ステップ S 241 でセキュリティモードオンの指示を受信したと判別したときには、C P U 201 は、家族情報メモリ 205 の記憶情報を参照して、在宅状況をチェックする(ステップ S 243)。そして、図 1
20 5 に示したテーブルを参照して、在宅状況に応じたセキュリティレベルを認識し、セキュリティモードオンにすることが可能であるか否か判別する(ステップ S 244)。

ステップ S 244 で、セキュリティモードオンにすることができないと判別したときには、C P U 201 は、その旨をドアロック制御装置 1
25 00 に通知する(ステップ S 245)。

一方、ステップ S 244 で、セキュリティモードオンにすることが可

能であると判別したときには、セキュリティモードをオンにすることができる旨をドアロック制御装置 100 に通知し（ステップ S 2 4 6）、所定時間経過するのを待つ（ステップ S 2 4 7）。

5 所定時間経過したことを確認したら、CPU 201 は、在宅状況に応じたセキュリティレベルでセキュリティモードをオンにする（ステップ S 2 4 8）。そして、セキュリティ監視動作を開始する（ステップ S 2 4 9）。

10 このセキュリティ監視動作中において、ドアロック制御装置 100 から識別情報を含む個人情報を受信したか否か判別し（ステップ S 2 5 0）、受信しなければステップ S 2 4 9 に戻って、セキュリティ監視動作を継続する。ドアロック制御装置 100 から個人情報を受信したと判別したときには、その結果としての在宅状況の変化をチェックし（ステップ S 2 5 1）、セキュリティレベルの変更が必要であるか判別する（ステップ S 2 5 2）。

15 セキュリティレベルの変更が必要ではないと判別したときには、CPU 201 は、ステップ S 2 4 9 に戻って、セキュリティ監視動作を継続する。また、ステップ S 2 5 2 で、セキュリティレベルの変更が必要であると判別したときには、変更の結果、セキュリティモードはオフにすべきものであるか否か判別し（ステップ S 2 5 3）、そうではないとき
20 には、在宅状況に応じてセキュリティレベルを変更する（ステップ S 2 5 4）。そして、セキュリティレベルを変更した旨をドアロック制御装置 100 に通知する（ステップ S 2 5 5）。

また、ステップ S 2 5 3 で、セキュリティモードはオフにすべきものであると判別したときには、セキュリティモードをオフにし（ステップ
25 S 2 5 6）、その旨をドアロック制御装置 100 に通知する（ステップ S 2 5 7）。そして、ステップ S 2 4 1 に戻る。

以上のようにして、この実施形態によれば、非接触の電子鍵装置を用いて、施錠、開錠を行なうので、鍵穴がなく、いわゆるピッキング対策の防犯効果がある。

また、電子鍵装置の所有者の生体情報により、電子鍵装置において、
5 当該電子鍵装置の使用者が所有者であるか否かについてのチェック（認証）を行ない、認証がOKであるときにのみ、電子鍵情報を送出するようにするので、電子鍵装置を紛失したとしても、所有者以外が電子鍵装置を使用して、ドアロック制御をすることは不可能であるので、セキュリティ上の安全性が非常に高い。

10 また、ドアロック装置2を、オートロックモードと、逐次ロックモードとで使い分けることができるので、使用者が、自分の使い勝手に合わせて、いずれのモードにするかを選択することができて、非常に便利である。

また、内側電子鍵リード／ライト部21inを設けて、この内側電子
15 鍵リード／ライト部21inによっても、ドアのロック状態を電子鍵装置により制御することができるので、窓などから侵入した不審者が玄関ドアから退出するのを妨げることができる。

また、内側電子鍵リード／ライト部21inと、外側電子鍵リード／
ライト部21exとを設けることにより、これらと電子鍵装置との通信
20 により、家族の入退出の管理をすることが容易である。

そのため、ドアロック装置2と、監視制御装置3とを組み合わせることにより、効率的なセキュリティ管理をすることができるようになる。
そして、セキュリティモードをドアロック時に設定できるようにしているので、従来は、家の中で設定して、所定時間後に、家の外に出なければ
25 ならないなどのあわただしさを解消することができる。

また、窓の閉め忘れがあったときには、ドアの開閉時に確認されるの

で、窓の閉め忘れを防止することができる。

また、家人の年齢、性別などにより、セキュリティモードのレベルを可変することができるようにしたので、在宅者が弱者である場合にも効果的なセキュリティレベルを設定することができる。また、ドアロック

5 の開錠、施錠に連携して、在宅状況の変化を把握することにより、セキュリティレベルの変更をすることができるというメリットもある。

[電子鍵情報の登録]

この電子鍵情報としての識別情報の登録が簡単にできることはセキュリティの点で好ましくないので、この例では、この電子鍵情報としての

10 識別情報の登録は、次のようにセキュリティを重視した方法により、例えばドアロック装置 2 の販売業者あるいは設置業者もしくは使用者により行なわれる。

まず、本鍵情報の登録について説明する。この実施形態においては、前述したように、初期的な本鍵情報となる識別情報を記憶する電子鍵装

15 置は、ICカードとしており、ドアロック装置 2 の販売業者あるいは設置業者から、ドアロック装置 2 の各戸への設置に際して、使用者に渡される。

この実施形態の場合、ドアロック装置 2 の各戸への設置前に、当該ドアロック装置 2 を設置する戸の家族構成員の各人についての個人情報が

20 収集される。そして、当該家族構成員の各人に対して、本鍵情報となる識別情報を記憶する IC カードが割り当てられ、それぞれの IC カードに記憶される本鍵情報としての識別情報と、前記収集された個人情報とからなる個人プロフィール情報が構成される。

そして、設置されるドアロック装置 2 のシリアル番号等からなる製品

25 番号、設置される住所、電話番号、ドアロック装置を利用する家族構成員の氏名などのユーザ情報と、各家族構成員の前記個人プロフィール情

報が、予め管理サーバ装置 10 のドアロック装置管理データベース 305 に、記憶される。すなわち、家族構成員それぞれの本鍵情報は、各家族構成員の個人プロフィール情報に含められて予め管理サーバ装置 10 に登録されている。

- 5 この際に、ドアロック装置管理データベースにおいては、家族構成員の個人プロフィール情報は、監視制御装置 3 の通信ネットワーク上のアドレス情報に対応して記憶される。当該アドレス情報としては、前述したように、この例では、電話番号や IP アドレスが用いられる。

- 10 管理サーバ装置 10 に登録された本鍵情報および各家族構成員の個人プロフィール情報は、ドアロック装置 2 の設置業者や販売業者が、ドアロック装置 2 の設置を完了したときに、管理会社の管理サーバ装置 10 に初期登録要求をしたときに、管理サーバ装置 10 から監視制御装置 3 に転送されることにより、監視制御装置 3 の家族情報メモリ 205 に書き込まれて登録される。また、監視制御装置 3 に登録された情報のうち、
15 少なくとも本鍵情報は、ドアロック制御装置 100 に転送されることにより、その家族情報メモリ 120 登録される。

図 34 は、初期登録要求を受けたときの管理サーバ装置 10 の動作を示すものである。図 34 の各ステップの動作は、主として CPU 301 が主体となって行なうものである。

- 20 先ず、CPU 301 は、初期登録要求を受け付けたか否か判別する（ステップ S261）。この初期登録要求は、ドアロック装置 2 のシリアル番号等の装置識別情報を伴ったものとされているもので、例えばパーソナルコンピュータなどから通信ネットワークを通じて管理サーバ装置 10 に送られる場合と、電話等で、初期登録要求を受けたオペレータが図
25 示しない入力手段により入力する場合とがある。

CPU 301 は、この初期登録要求を受け取ると、装置識別情報を検

5 索子として、ドアロック装置データベースを検索し、予め登録されている
ドアロック装置 2 および監視制御装置 3 の通信ネットワーク 9 上での
アドレス情報を読み出して、初期登録要求を含む発呼をする。つまり、
初期登録要求されたドアロック装置 2 が接続されている監視制御装置 3
に対して初期登録要求の発呼を行なう（ステップ S 2 6 2）。

このとき、監視制御装置 3 は、自動応答を行なうので、CPU 3 0 1
は、当該監視制御装置 3 からの応答を確認して、当該監視制御装置 3 と
の間に通信路を形成する（ステップ S 2 6 3）。

10 次に、CPU 3 0 1 は、ドアロック装置 2 に関連して上述のように管
理サーバ装置 1 0 のドアロック装置データベース 2 0 5 に記憶している、
ドアロック装置が設置された家の家族構成員全員についての本鍵情報
を含む個人プロフィール情報を監視制御装置 3 に送信する（ステップ S 2
6 4）。

15 次に、CPU 3 0 1 は、監視制御装置 3 に送信すべき情報が全部終了
し終わり、監視制御装置 3 から登録完了通知が到来するのを待ち（ステ
ップ S 2 6 5）、登録完了通知を受け取ったと判別したときには、監視
制御装置 3 との通信路を切断して（ステップ S 2 6 6）、この初期登録
の処理ルーチンを終了する。

20 この初期登録要求情報を受け取る監視制御装置 3 の動作を、図 3 5 の
フローチャートを参照して説明する。

監視制御装置 3 の CPU 2 0 1 は、管理サーバ装置 1 0 からの着信を
受信したか否か判別し（ステップ S 2 7 1）、管理サーバ装置 1 0 から
の着信の受信でなかったと判別したときには、その他の処理を行なう（ス
テップ S 2 7 2）。

25 管理サーバ装置 1 0 からの着信を受信したと判別したときには、CPU
2 0 1 は、その着信に自動応答して管理サーバ装置 1 0 との間に通信

路を形成する（ステップS 2 7 3）。そして、受信した着信は初期登録要求であるか否か判別する（ステップS 2 7 4）。初期登録要求であると判別すると、CPU 2 0 1は、管理サーバ装置1 0からの登録情報を待ち、登録情報を受信したら（ステップS 2 7 5）、受信した登録情報を、家族情報メモリ2 0 5に書き込む（ステップS 2 7 6）。

そして、家族全員についての登録情報の書き込みが完了したら、管理サーバ装置1 0に登録完了通知を返送し（ステップS 2 7 7）、管理サーバ装置1 0との通信路を切断する（ステップS 2 7 8）。

次に、CPU 2 0 1は、家族情報メモリ2 0 5に書き込んで登録した個人プロフィール情報のうち、少なくとも家族構成員のそれぞれについての本鍵情報である識別情報をドアロック制御装置1 0 0に転送する（ステップS 2 7 9）。ドアロック制御装置1 0 0は、この情報を受けて、家族情報メモリ1 2 0に受信した本鍵情報を登録する。本鍵情報としての識別情報のほかに、家族構成員についての個人情報の必要なものをも、ドアロック制御装置1 0 0に転送するようにしてもよいことは言うまでもない。なお、ドアロック制御装置1 0 0での登録動作は、上述の監視制御装置での鍵登録動作と同様であるので、ここでは省略する。

そして、CPU 2 0 1は、ドアロック制御装置1 0 0への本鍵情報および必要は情報の転送の終了を確認すると（ステップS 2 8 0）、この処理ルーチンを終了する。

なお、ステップS 2 7 4で、初期登録ではないと判別したときには、CPU 2 0 1は、バックアップ鍵の登録要求であるか否か判別し（ステップS 2 8 1）、バックアップ鍵の登録要求であると判別したときには、当該バックアップ登録の処理を実行する（ステップS 2 8 2）。このバックアップ登録の処理の詳細説明はこの明細書では省略する。

また、ステップS 2 8 1でバックアップ登録要求ではないと判別した

ときには、CPU 201は、紛失鍵の抹消要求であるか否か判別する（ステップS 283）。そして、紛失鍵の抹消要求でないと判別したときには、CPU 201は、その他の処理を実行し（ステップS 284）、紛失鍵の抹消要求であると判別したときには、当該抹消要求の処理を実行する（ステップS 285）。この抹消処理についての詳細説明はこの明細書では省略する。以上で、図35の処理を終了する。

[通知連絡設定]

次に、この実施形態では、ユーザは、監視制御装置3に対して、予め、帰宅予定者、外出予定者、帰宅予定時刻、外出予定時刻、通知連絡者などを設定することができ、監視制御装置3は、それら設定された情報を通知連絡設定メモリ222に記憶する。そして、後述するように、監視制御装置3は、設定された帰宅予定時刻や外出予定時刻を監視して、設定された帰宅予定者、設定された外出予定者、設定された通知連絡者に、当該帰宅予定者、当該外出予定者の入退出に関する情報、つまり、帰宅、外出に関する情報を通知連絡するようにする。

先ず、帰宅予定者、外出予定者、帰宅予定時刻、外出予定時刻、通知連絡者などの設定処理について、図36および図37のフローチャートを参照して説明する。

先ず、監視制御装置3のCPU 201は、リモコン受信部38の受信信号を監視して、リモートコマンド50でボタン操作されたか否か判別する（ステップS 291）。このステップS 291で、ボタン操作されないと判別されたときには、その他の処理を行なう（ステップS 292）。

ステップS 291で、リモートコマンド50でボタン操作がされたと判別したときには、CPU 201は、リモートコマンド50で操作されたボタンは、メニューボタン55であるか否か判別する（ステップS 293）。メニューボタン55ではないと判別したときには、CPU 20

1 は、操作されたボタンに対応する処理を実行する(ステップ S 2 9 4)。

また、ステップ S 2 9 3 で、操作されたボタンがメニューボタン 5 5 であると判別したときには、CPU 2 0 1 は、テレビ受像機 7 に電源が投入されていないときには、テレビ受像機 7 の電源をオンにして(ステップ S 2 9 5)、メニューの一覧をテレビ受像機 7 の画面に、前述の伝言記録再生の場合と同様にして表示するようにする(ステップ S 2 9 6)。

このメニューの一覧表示に対しては、操作者は、行ないたい設定メニュー項目の選択をリモートコマンド 5 0 のカーソルキーを用いて行なう。CPU 2 0 1 は、リモコン受信部 3 8 の受信信号を監視してメニュー項目の選択操作がなされたか否か判別し(ステップ S 2 9 7)、メニュー項目の選択操作がなされたと判別したときには、例えば反転表示して示す選択中項目を、選択操作に応じて変更する(ステップ S 2 9 8)。そして、設定項目の決定操作がなされたか否か判別する(ステップ S 2 9 9)。

また、ステップ S 2 9 7 で、メニュー項目の選択操作がなされないと判別したときには、CPU 2 0 1 は、即座にステップ S 2 9 9 に進んで設定項目の決定操作がなされたか否か判別する。そして、ステップ S 2 9 9 で、設定項目の決定操作がなされないと判別したときには、ステップ S 2 9 7 に戻る。

また、ステップ S 2 9 9 で、設定項目の決定操作がなされたと判別したときには、CPU 2 0 1 は、選択された設定項目は帰宅予定に関する通知の設定であるか否か判別し(図 3 7 のステップ S 3 0 1)、そうではなかったときには選択された設定項目は外出予定に関する通知の設定であるか否か判別する(ステップ S 3 0 3)。そして、外出予定に関する通知の設定ではないと判別したときには、その他の設定項目についての処理ルーチンを実行する(ステップ S 3 0 5)。

ステップS 3 0 1で、帰宅予定に関する通知の設定であると判別したときには、CPU 2 0 1は、帰宅予定時刻、帰宅予定者、帰宅通知連絡者などの設定用画面をテレビ受像機7の画面に表示する（ステップS 3 0 2）。この例の場合、設定用画面においてユーザに対して設定要求される帰宅通知連絡者は、帰宅予定者本人以外とされる。しかし、後述するように、帰宅予定に関する通知の設定がなされた場合には、監視制御装置3では、帰宅予定時刻になっても帰宅しない帰宅予定者に帰宅を促す通知を帰宅予定者に送るようにするので、実際の帰宅通知連絡者には、当該帰宅予定者本人が予め含まれるものとなる。

- 10 ステップS 3 0 2の次のステップS 3 0 6において、CPU 2 0 1は、帰宅予定に関する通知について、すべての設定項目の設定入力終了したか否かを判別し（ステップS 3 0 6）、すべての設定入力終了したと判別したときには、設定された項目情報を、通知連絡設定メモリ222に書き込み（ステップS 3 0 7）、その後、テレビ受像機7の電源をオフして（ステップS 3 0 8）、この設定処理ルーチンを終了する。

- 20 また、ステップS 3 0 3で、外出予定に関する通知の設定であると判別したときには、CPU 2 0 1は、外出予定時刻、外出予定者、外出通知連絡者などの設定用画面をテレビ受像機7の画面に表示する（ステップS 3 0 4）。この例の場合、設定用画面においてユーザに設定要求される外出通知連絡者は、外出予定者本人以外とされる。しかし、後述するように、外出予定に関する通知の設定がなされた場合には、監視制御装置3では、外出予定時刻になっても外出しない外出予定者に外出を促す通知を外出予定者に送るようにするので、実際の外出通知連絡者には、当該外出予定者本人が予め含まれるものとなる。

- 25 そして、ステップS 3 0 4の次のステップS 3 0 6において、CPU 2 0 1は、外出予定に関するすべての設定項目についての設定入力終了

了したか否か判別し（ステップS 3 0 6）、すべての設定入力終了したと判別したときには、設定された項目情報を、通知連絡設定メモリ 2 2 2 に書き込み（ステップS 3 0 7）、その後、テレビ受像機 7 の電源をオフして（ステップS 3 0 8）、この設定処理ルーチンを終了する。

5 〔通知連絡処理〕

次に、以上のようにして帰宅予定または外出予定に関する通知設定がなされたときの、監視制御装置 3 における通知連絡の動作を、図 3 8 ～ 図 4 0 を参照して説明する。

まず、監視制御装置 3 は、帰宅または外出に関する通知連絡の待機状態となっている（ステップS 3 1 0）。この待機状態においては、セキュリティモードオン状態であってもよいし、また、セキュリティモードオフの状態であってもよい。

この待機状態において、CPU 2 0 1 は、ドアロック制御装置 1 0 0 からの情報を受信したか否か判別する（ステップS 3 1 1）。そして、
15 ドアロック制御装置 1 0 0 からの情報を受信したと判別したときには、CPU 2 0 1 は、受信した情報は、帰宅者情報であるか外出者情報であるかを判別する（ステップS 3 1 2）。

ステップS 3 1 2 において、受信した情報は外出者情報であると判別したときには、CPU 2 0 1 は、通知連絡設定メモリ 2 2 2 に記憶されている外出予定者の識別情報と、ドアロック制御装置 1 0 0 から受信した外出者情報に含まれる外出者の識別情報とを比較し、その比較結果に基づき、外出者は設定された外出予定者であるか否か判別し（ステップ
20 S 3 1 3）、外出予定者でなければ、ステップS 3 1 0 に戻り、待機状態になる。

25 また、ステップS 3 1 3 において、外出者は設定された外出予定者であると判別したときには、CPU 2 0 1 は、通知連絡設定メモリ 2 2 2

に記憶されている外出通知連絡者の情報を読み出す。そして、この例においては、家族情報メモリ 205 に記憶されている外出通知連絡者の個人情報を検索して、そのメールアドレスを読み出し、当該外出通知連絡者の例えば携帯電話端末に対して、設定された外出予定者が外出したことを電子メールにより通知連絡する（ステップ S 3 1 4）。この通知連絡には、外出した時刻の情報も含まれる。

そして、通知連絡をした後、CPU 201 は、通知連絡設定メモリ 222 に記憶されている当該外出予定に関する通知についての設定情報を消去して（ステップ S 3 1 5）、この処理ルーチンを終了する。

10 以上により、例えば、外出している親が、外出予定者として設定した子供が、予定の時刻に外出したかどうかを知ることができる。

ステップ S 3 1 2 で、ドアロック制御装置 100 から受信した情報が帰宅者情報であると判別したときには、CPU 201 は、通知連絡設定メモリ 222 に記憶されている帰宅予定者の識別情報と、ドアロック制御装置 100 から受信した帰宅者情報に含まれる帰宅者の識別情報とを比較し、その比較結果に基づき、帰宅者は設定された帰宅予定者であるか否かを判別し（ステップ S 3 1 6）、帰宅予定者でなければ、ステップ S 3 1 0 に戻り、待機状態になる。

また、ステップ S 3 1 6 において、帰宅者は設定された帰宅予定者であると判別したときには、CPU 201 は、通知連絡設定メモリ 222 に記憶されている帰宅通知連絡者の情報を読み出す。そして、この例においては、家族情報メモリ 205 に記憶されている外出通知連絡者の個人情報を検索して、そのメールアドレスを読み出し、当該外出通知連絡者の例えば携帯電話端末に対して、当該帰宅通知連絡者に、設定された帰宅予定者が帰宅したことを電子メールにより通知連絡する（ステップ S 3 1 7）。この通知連絡には、帰宅した時刻の情報も含まれる。

そして、通知連絡をした後、CPU 201は、通知連絡設定メモリ 222に記憶されている当該帰宅予定に関する通知についての設定情報を消去して（ステップS 315）、この処理ルーチンを終了する。

5 以上により、例えば、外出している親が、帰宅予定者として設定した子供が、予定の時刻に帰宅したかどうかを知ることができる。

次に、ステップS 311において、ドアロック制御装置100からの情報を受信してはいないと判別したときには、CPU 201は、通知連絡設定メモリ 222に記憶されている帰宅予定時刻と時計回路 221が示す現在時刻とを比較し、帰宅予定時刻を経過したか否か判別する（ス
10 テップS 318）。

ステップS 318で、帰宅予定時刻は経過していないと判別したときには、CPU 201は、通知連絡設定メモリ 222に記憶されている外出予定時刻と時計回路 221が示す現在時刻とを比較し、外出予定時刻を経過したか否か判別する（ステップS 319）。ステップS 319で、
15 現在時刻が外出予定時刻も経過していないと判別したときには、ステップS 310に戻り、待機状態になる。

ステップS 318において、現在時刻が帰宅予定時刻を経過していると判別したときには、CPU 201は、帰宅予定者に帰宅を促す通知連絡を行なう（図39のステップS 321）。すなわち、家族情報メモリ
20 205に記憶されている帰宅予定者のメールアドレスを読み出し、例えば、当該帰宅予定者の携帯電話端末に電子メールにより、速やかに帰宅すべき旨の通知を行なって、帰宅を促すようにする。

次に、CPU 201は、通知連絡設定メモリ 222に記憶されている帰宅通知連絡者の情報を読み出し、家族情報メモリ 205に記憶されて
25 いる当該帰宅通知連絡者の個人情報を検索して、そのメールアドレスを読み出し、当該帰宅通知連絡者の例えば携帯電話端末に対して、設定さ

れた帰宅予定者が未だ帰宅していないことを電子メールにより通知連絡する（ステップS 3 2 2）。

その後、CPU 2 0 1 は、ドアロック制御装置 1 0 0 からの帰宅者情報を待ち（ステップS 3 2 3）、また、帰宅者情報を受信せずに所定時間、例えば 1 0 分、経過したか否かを判別し（ステップS 3 2 4）、所定時間経過していないと判別したときには、ステップS 3 2 3 に戻って、帰宅者情報の到来を待つ。また、ステップS 3 2 4 で所定時間経過したと判別したときには、ステップS 3 2 1 に戻り、再度、帰宅予定者に帰宅を促す電子メールを送る。

10 また、ステップS 3 2 3 でドアロック制御装置 1 0 0 から帰宅者情報を受信したと判別したときには、CPU 2 0 1 は、ドアロック制御装置 1 0 0 からの帰宅者情報に含まれる識別信号により識別される帰宅者は、設定された帰宅予定者であるか否かを判別する（ステップS 3 2 5）。このステップS 3 2 5 で、帰宅者が設定された帰宅予定者でないと判別したときには、CPU 2 0 1 は、ステップS 3 2 4 に進んで、所定時間の経過を待ち、ステップS 3 2 4 以降の上述の動作を繰り返す。

20 ステップS 3 2 5 で判別された帰宅者が予め設定された帰宅予定者であると判別したときには、CPU 2 0 1 は、家族情報メモリ 2 0 5 に記憶されている帰宅通知連絡者の個人情報を検索して、そのメールアドレスを読み出し、当該帰宅通知連絡者の例えば携帯電話端末に対して、当該帰宅通知連絡者に、設定された帰宅予定者が帰宅したことを電子メールにより通知連絡する（ステップS 3 1 7）。この通知連絡には、帰宅した時刻の情報も含まれる。

25 そして、通知連絡をした後、CPU 2 0 1 は、通知連絡設定メモリ 2 2 2 に記憶されている当該帰宅予定者に関する設定情報を消去して（ステップS 3 1 5）、この処理ルーチンを終了する。

また、ステップ S 3 1 9 において、現在時刻が外出予定時刻を経過していると判別したときには、CPU 2 0 1 は、外出予定者に外出を促す通知連絡を行なう（図 4 0 のステップ S 3 3 1）。すなわち、家族情報メモリ 2 0 5 に記憶されている外出予定者のメールアドレスを読み出し、

5 当該外出予定者の例えば携帯電話端末に、電子メールにより、速やかに外出すべき旨の通知を行なって、外出を促すようにする。これにより、外出予定者は、他事に忙殺されていたとしても、所定の外出予定時刻に外出することが可能となる。

次に、CPU 2 0 1 は、通知連絡設定メモリ 2 2 2 に記憶されている

10 外出通知連絡者の情報を読み出し、家族情報メモリ 2 0 5 に記憶されている当該外出通知連絡者の個人情報を参照して、そのメールアドレスを読み出し、当該外出通知連絡者の例えば携帯電話端末に対して、設定された外出予定者が未だ外出していないことを電子メールにより通知連絡する（ステップ S 3 3 2）。

15 この通知連絡を受けた外出通知連絡者は、自宅に電話をかけるなどして、外出予定者に外出を促すことができる。外出予定者は、自分の携帯電話に電源が投入されていないなどの理由で、ステップ S 3 3 1 で通知連絡を受けない場合においても、外部からの外出通知連絡者による電話連絡などにより促されて、外出予定時刻に外出することが可能になる。

20 その後、CPU 2 0 1 は、ドアロック制御装置 1 0 0 からの外出者情報を待ち（ステップ S 3 3 3）、また、外出者情報を受信せずに所定時間、例えば 1 0 分、経過したか否かを判別し（ステップ S 3 3 4）、所定時間経過していないと判別したときには、ステップ S 3 3 3 に戻って、外出者情報の到来を待つ。また、ステップ S 3 3 4 で所定時間経過した

25 と判別したときには、ステップ S 3 3 1 に戻り、再度、外出予定者に外出を促す電子メールを送る。

また、ステップ S 3 3 3 でドアロック制御装置 1 0 0 から外出者情報を受信したと判別したときには、CPU 2 0 1 は、外出者情報が含む識別信号により識別される外出者は、設定された外出予定者であるか否か判別する（ステップ S 3 3 5）。このステップ S 3 3 5 で、外出者が設定された外出予定者でないと判別したときには、CPU 2 0 1 は、ステップ S 3 3 4 に進んで、所定時間の経過を待ち、ステップ S 3 3 4 以降の上述の動作を繰り返す。

ステップ S 3 3 5 で判別された外出者が予め設定された外出予定者であると判別したときには、CPU 2 0 1 は、家族情報メモリ 2 0 5 に記憶されている外出通知連絡者の個人情報を検索して、そのメールアドレスを読み出し、当該外出通知連絡者の例えば携帯電話端末に対して、当該外出通知連絡者に、設定された外出予定者が外出したことを電子メールにより通知連絡する（ステップ S 3 1 4）。この通知連絡には、外出した時刻の情報も含まれる。

そして、通知連絡をした後、CPU 2 0 1 は、通知連絡設定メモリ 2 2 2 に記憶されている当該外出予定者に関する設定情報を消去して（ステップ S 3 1 5）、この処理ルーチンを終了する。

以上のようにして、この実施形態によれば、例えば親が、子供を帰宅予定者として設定すると共に、帰宅予定時刻を設定し、さらに、当該親を帰宅通知連絡者に設定しておくことにより、親は、子供が予定された帰宅時刻に帰宅しているかどうかを確認することができると共に、子供に速やかな帰宅を促すことができる。

また、外出を予定している者が、外出予定時刻を設定しておくことにより、外出予定時刻を失念してしまっても、外出予定時刻になると外出を促すようにされるので、確実に予定した時刻に外出することが可能になる。

〔他の実施形態〕

上述の実施形態では、所定の予約設定時刻になったときに、帰宅予定者や外出予定者、および予め設定した帰宅通知連絡者、外出通知連絡者に、帰宅予定者や外出予定者の帰宅状況、外出状況を通知連絡するよう
5 にしたが、ドアロック制御装置 100 と、電子鍵装置との通信を行なって、外出あるいは帰宅する者についての情報を、予め設定した通知連絡者に通知連絡するようにしても勿論よい。

また、以上の実施形態では、通信装置は、ドアロック装置 2 とセキュリティシステムの監視制御装置 3 とを含む構成としたが、ドアの施錠お
10 よび開錠のみを目的とするドアロック制御システムとして考えた場合には、監視制御装置 3 は不要であって、通信装置は、ドアロック装置 2 のみで構成することもできる。その場合には、ドアロック装置 2 は、電話回線を通じて携帯電話端末にメールや電話をかける機能を備えるものである。

15 また、通知連絡の方法は、電子メールとしたが、音声合成などを用いることにより、電話を携帯電話端末や予め定められた電話番号の固定電話端末にかけて、音声情報として、帰宅や外出を促す通知や、帰宅状況や外出状況を通知するようにすることもできる。

また、上述の実施形態では、電子鍵情報を IC チップの製造番号とし、
20 これと個人情報とを対応させることにより、電子鍵情報を個人識別情報としても用いるようにしたが、電子鍵情報と共に、予め個人識別情報を定めて電子鍵装置や、ドアロック制御装置、監視制御装置などに登録しておき、電子鍵装置と、リード／ライト部との通信の際に電子鍵情報と共に、個人識別情報をやり取りするようにしてもよい。その場合には、
25 電子鍵情報のほかに、各個人ごとに識別情報が設定され、それが電子鍵装置のメモリに記憶されると共に、ドアロック制御装置や監視制御装置

のメモリの個人プロフィール情報に含められて記憶される。

そのように個人識別情報を電子鍵情報と別個とする場合には、一つの
ドアロック装置に一つの電子鍵情報として、当該家に住む家族構成員の
全員に共通の一つの電子鍵情報を用いるようにして、各人が、その共通
5 鍵情報を格納する電子鍵装置をそれぞれ持つようにすることもできる。

また、上述の実施形態では、通知連絡者への連絡のための情報、例え
ば電子メールアドレスや、電話番号あるいはパーソナルコンピュータに
通知する場合にはIPアドレスは、監視制御装置やドアロック制御装置
に予め記憶されている情報を読み出して用いるようにしたが、電子鍵装
10 置との通信時に電子鍵装置から取得するように構成してもよい。

上述の実施形態は、セキュリティ監視システムも含む通信システムの
構成であったので、管理サーバ装置10が存在しているが、セキュリティ
監視システムが存在しない通信システムの構成も可能である。

なお、電子鍵情報は、管理サーバ装置からドアロック装置の電子鍵情
15 報の記憶部に転送して、登録するのではなく、住戸に設置する前に、予
め、ドアロック装置に登録して記憶しておくようにしても勿論よい。特
に、上述の実施形態のようなセキュリティ監視システムを用いずに、ド
アロック制御システムを単独で使用するような場合には、そのようにす
るものである。

20 また、ICチップのメモリには、予め一元管理された識別情報が記憶
されているように説明したが、後から、一元管理されている識別情報が
書き込まれるようにされてもよいことは言うまでもない。

なお、上述の実施形態では、電子鍵装置を、外側電子鍵リード／ライ
ト部21exに対して、ドアの施錠後、所定時間以内にかざした場合に、
25 セキュリティモードをオンにするようにしたが、ドアロック制御装置1
00または監視制御装置3では、玄関ドア1からの入退出を管理してい

るので、在宅者が無くなったら、自動的にセキュリティレベルAでセキュリティモードをオンにするようにすることもできる。

その場合に、ドアロック制御装置100で、在宅者無しを検出したときに、監視制御装置3にセキュリティモードオンを要求しても良いし、
5 監視制御装置3が、自装置で、在宅者無しを検出したときに、セキュリティモードオンとするようにしても良い。

なお、この例では、在宅者が玄関ドア1を開錠し、玄関ドア1を開けたときには、それまでにセキュリティモードがオンになっていても、一旦、セキュリティモードは、オフとされるものとしたが、セキュリティ
10 モードがオンになっているときに外出者があった場合には、外出者を電子鍵装置との通信により取得される識別情報により認識して、監視制御装置3が、帰宅者があった場合と全く同様にして、在宅状況の変化に対応して自動的にセキュリティレベルを変更するようにすることもできる。

なお、以上の実施形態の説明では、鍵情報としての識別情報の認証は、
15 ドアロック装置で行なうようにしたが、ドアロック装置2は、監視制御装置3に、あるいは監視制御装置3を介して管理サーバ装置10に鍵情報を送り、監視制御装置3あるいは管理サーバ装置10で、認証作業を行ない、その認証結果を、ドアロック装置2に返す（管理サーバ装置10の場合には監視制御装置3を介して返す）ようにしても良い。その場
20 合には、監視制御装置3からドアロック制御装置100への鍵情報の転送や抹消指示を送る必要はない。

また、開錠者、施錠者の識別情報も監視制御装置3ではなく、管理サーバ装置10に送り、管理サーバ装置10により、セキュリティ管理をするようにしてもよい。

25 また、以上の説明では、外出者か帰宅者かは、ドアロック制御装置100で判別するようにしたが、監視制御装置3においても、ドアロック

制御装置 100 でのドアロック制御モードの設定情報を備えているので、
ドアロック制御装置 100 は、IC カード 40 F が、内側電子鍵リード
／ライト部 21 i n または外側電子鍵リード／ライト部 21 e x にかざ
されて通信が両者の間で行なわれ、識別情報についての認証がとれたと
5 きには、その識別情報と、内側電子鍵リード／ライト部 21 i n または
外側電子鍵リード／ライト部 21 e x のいずれと通信したかの情報と、
開錠か施錠かの情報とを、監視制御装置 3 に送り、監視制御装置 3 が、
外出か帰宅かを判別するようにすることもできる。

10 なお、電子鍵装置は、上述もしたように、IC カードに限られるもの
ではなく、上述の例の場合であれば、IC カードと同様の IC チップや、
通信手段および生体情報の取得手段などを備える携帯電話端末や PDA
(携帯情報端末) などを用いることができるものである。

また、電子鍵装置は、上述の実施形態のような非接触形式で電子鍵情
報の通信を行なうのものに限られるものではなく、接触形式で電子鍵情
15 報の通信を行なうものであっても勿論よい。

産業上の利用可能性

以上説明したように、この発明による通信装置によれば、ドアの施錠、
開錠を行なう個人を管理することにより、帰宅予定者や外出予定者に帰
20 宅や外出を促すことができると共に、帰宅状況や外出状況を、外出中の
通知連絡者に通知連絡することが可能になる。

請 求 の 範 囲

1. 少なくとも電子鍵情報を記憶する電子鍵装置と通信を行なう第1の通信手段と、

5 通信ネットワークを通じて情報送信を行なうための第2の通信手段と、
電子鍵情報を記憶する記憶部と、

前記第1の通信手段を通じて前記電子鍵装置から受信する電子鍵情報と、前記記憶部に記憶されている電子鍵情報とを比較し、その比較結果に基づいてドアのロック機構を制御するドアロック制御手段と、

10 前記第1の通信手段を通じて前記電子鍵装置から受信した情報に基づいて当該電子鍵装置の利用者を認識する利用者認識手段と、

前記利用者認識手段での認識結果に基づいて、前記電子鍵装置の利用者の入退出に関する情報を、予め定められている通知先に前記第2の通信手段を介して送信するように制御する送信制御手段と、

15 を備えることを特徴とする通信装置。

2. 請求項1に記載の通信装置において、

前記通知先に入退出に関する情報を送信すべき前記電子鍵装置の利用者の設定を受け付けて記憶する設定記憶手段を備え、

前記送信制御手段は、前記設定された前記電子鍵装置の利用者の入退出に関する情報を、前記第2の通信手段を介して前記通知先に送信することを特徴とする通信装置。

3. 請求項2に記載の通信装置において、

前記設定記憶手段では、前記電子鍵装置の利用者と共に、当該利用者に対応して時刻情報の設定入力を受け付けて記憶し、

25 前記送信制御手段は、前記設定入力された時刻情報に対応する時刻を経過しても、前記利用者認識手段で前記設定された前記電子鍵装置の使

用者を認識しなかったときに、当該電子鍵装置の使用者の入退出がなされていないことに関する情報を、前記通知先に前記第2の通信手段を介して送信するように制御する

ことを特徴とする通信装置。

5 4. 請求項3に記載の通信装置において、

前記通知先は、前記設定された前記電子鍵装置の使用であり、前記電子鍵装置の使用の入退出がなされていないことに関する情報は、前記入退出を促す情報である

ことを特徴とする通信装置。

10 5. 請求項3に記載の通信装置において、

前記通知先は、前記設定された前記電子鍵装置の使用以外である

ことを特徴とする通信装置。

6. 請求項5に記載の通信装置において、

15 前記設定された時刻情報に対応する時刻の経過後に、前記使用者認識手段で前記設定された前記電子鍵装置の使用を認識したときに、当該電子鍵装置の使用の入退出に関する情報を、前記通知先に前記第2の通信手段を介して送信するように制御する

ことを特徴とする通信装置。

7. 請求項1に記載の通信装置において、

20 前記電子鍵情報は、前記電子鍵装置の使用を識別することが可能な識別情報で構成され、

前記使用者認識手段は、前記電子鍵装置から受信した前記電子鍵情報に基づいて前記ドアから入退出した前記電子鍵装置の使用を認識することを特徴とする通信装置。

25 8. 請求項1に記載の通信装置において、

前記電子鍵情報は、同一のものが存在しないように一元管理されて割

り振られた識別情報であり、

前記電子鍵情報に対応して前記電子鍵装置の所有者を特定可能とする
個人情報記憶する個人情報記憶部を備えるとともに、前記電子鍵装置
から受信した前記電子鍵情報と、前記記憶部に記憶されている電子鍵情
5 報とを比較し、その比較結果に基づいて、前記電子鍵装置の所有者の前
記ドアからの入退出を管理する手段を備えると共に、

前記使用者認識手段は、前記電子鍵装置から受信した前記電子鍵情報
に基づいて前記ドアから入退出した前記電子鍵装置の使用者を認識する
ことを特徴とする通信装置。

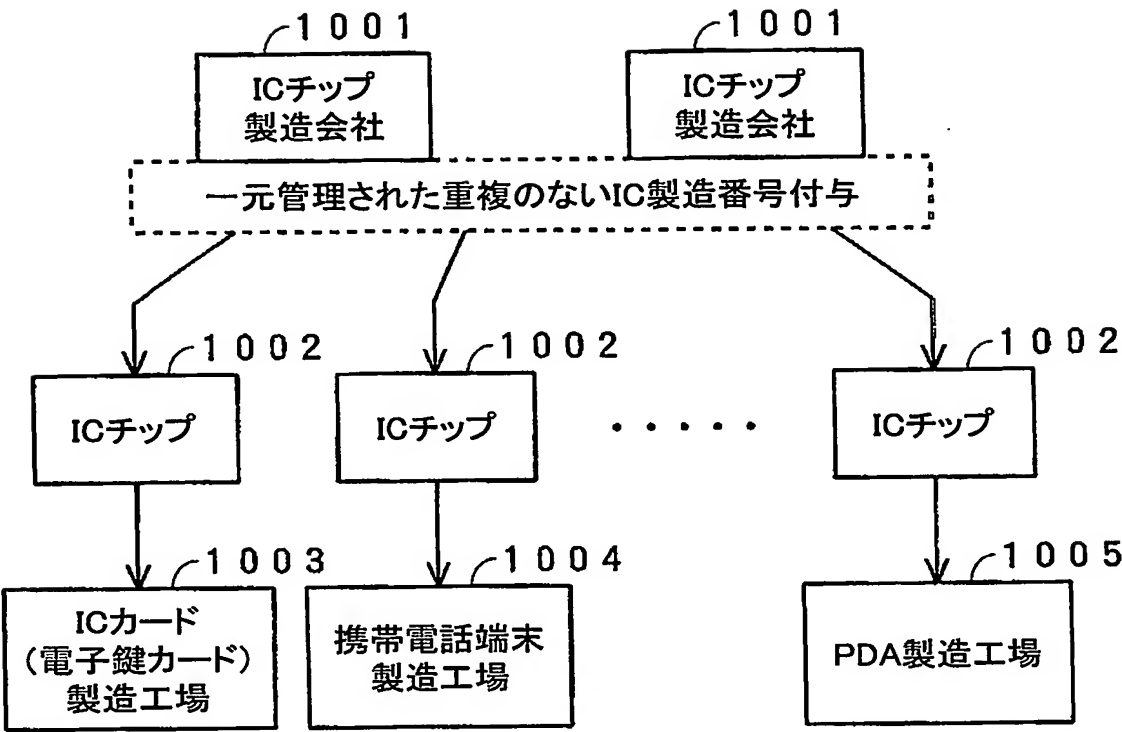


Fig.1



Fig.2

2/38

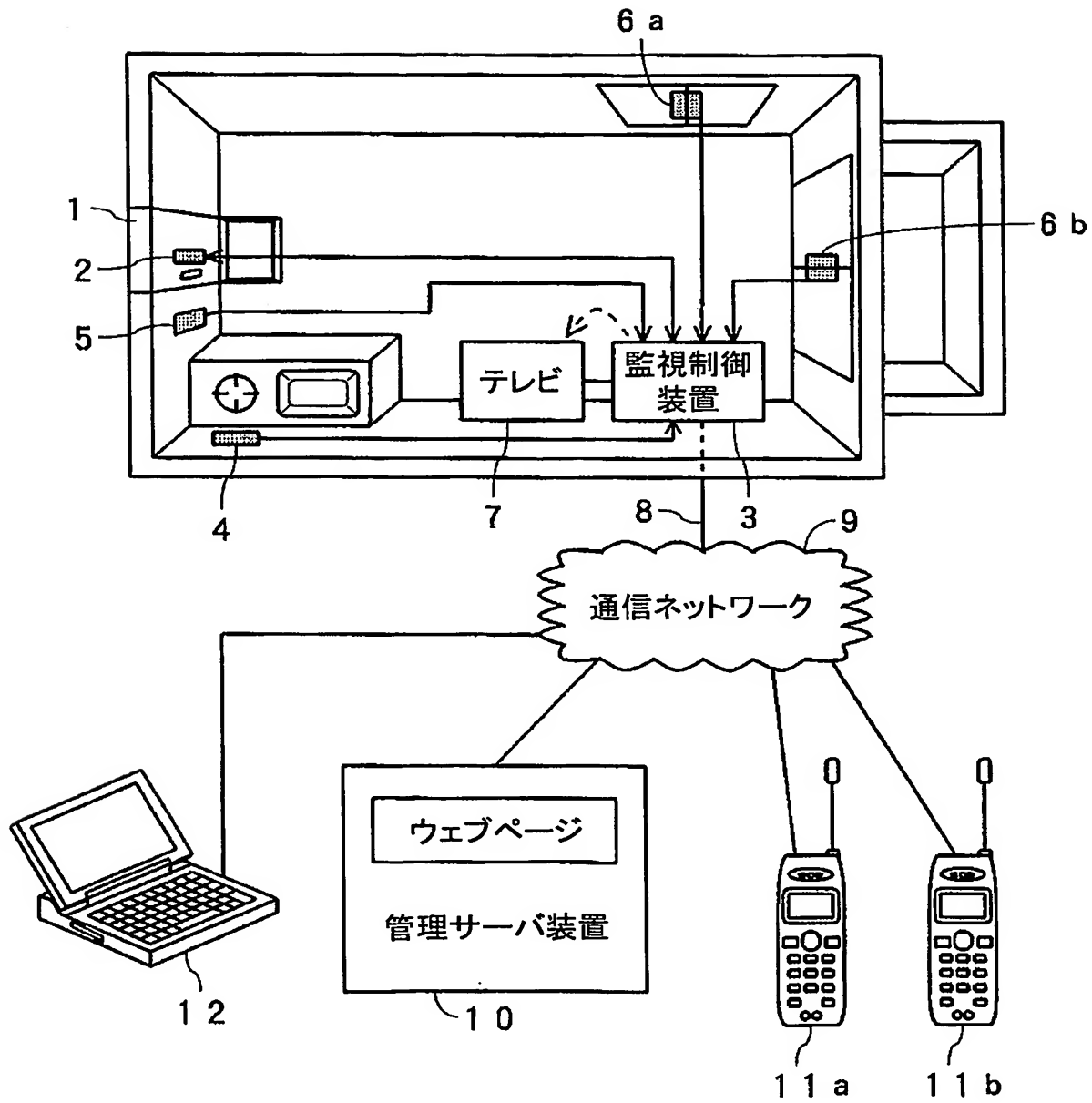


Fig.3

3/38

Fig.4A

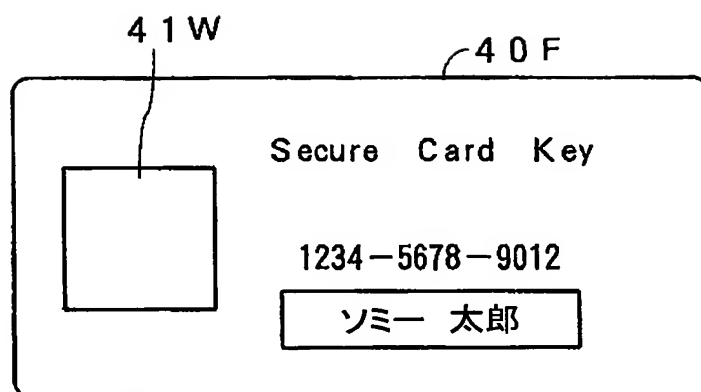
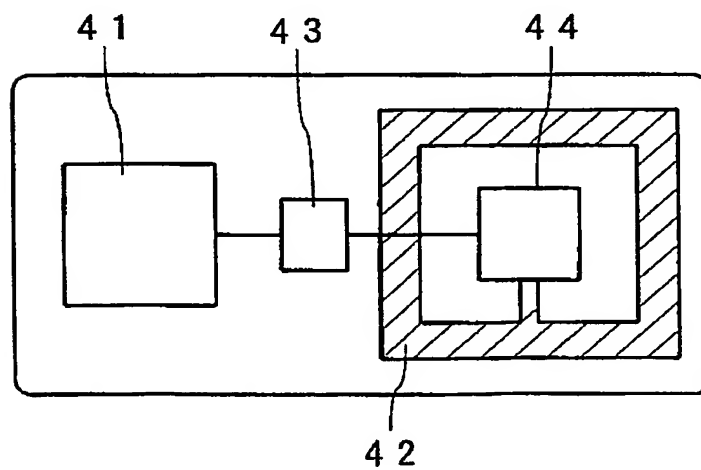


Fig.4B



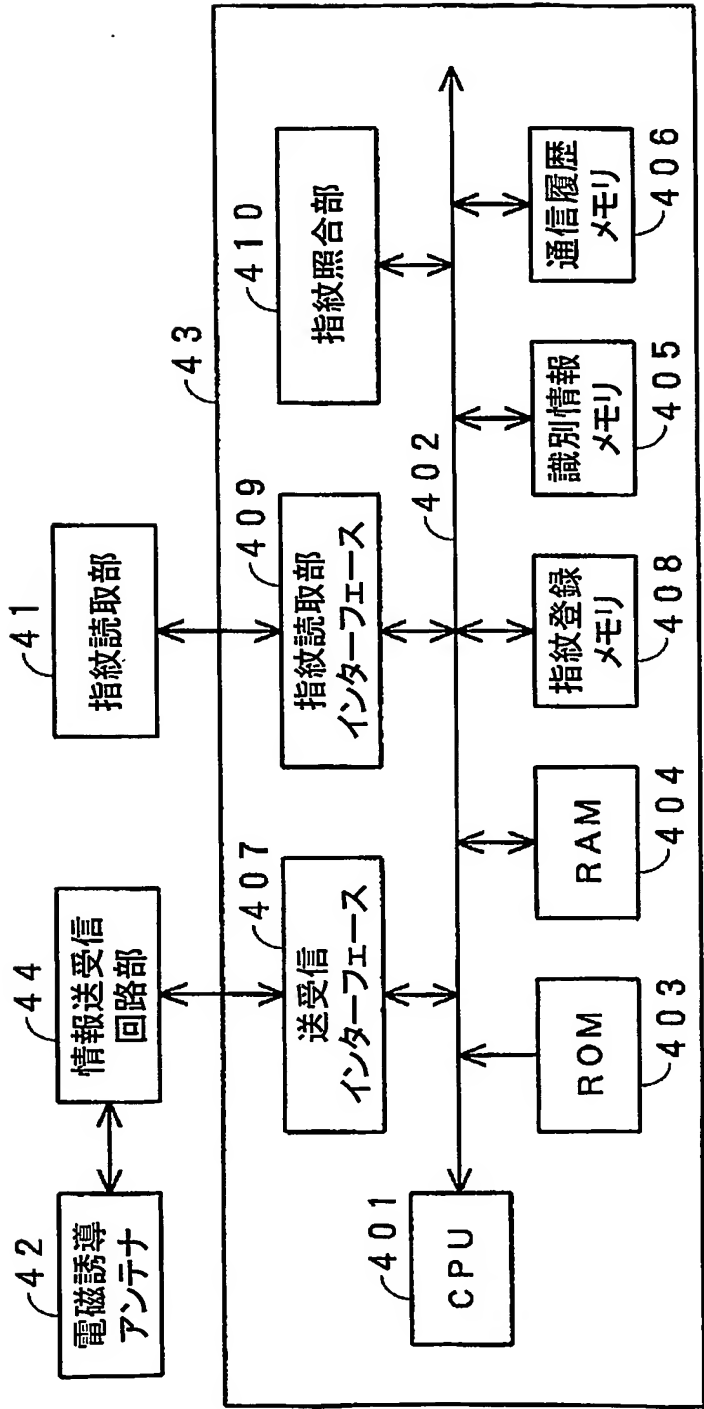


Fig.5

5/38

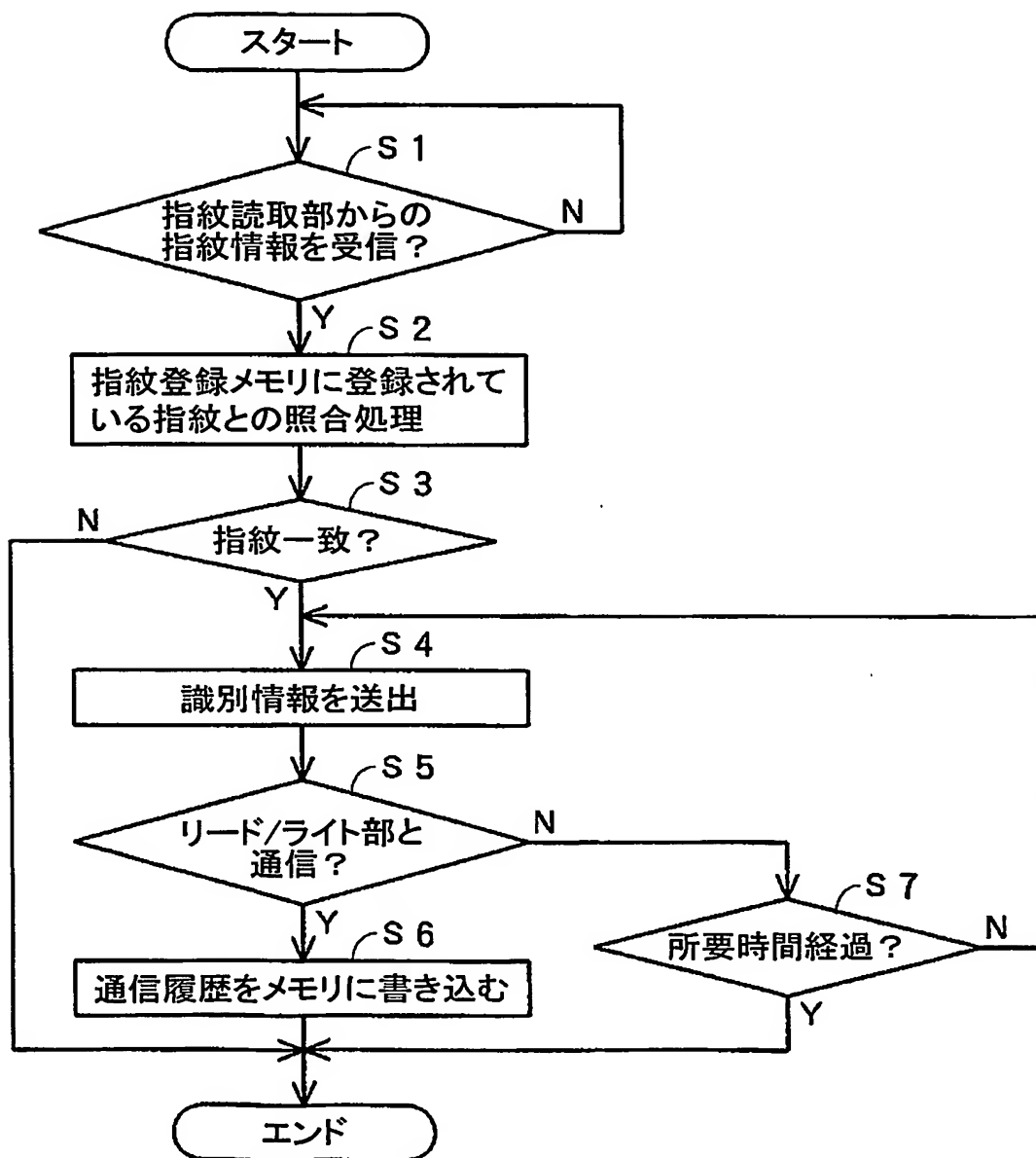


Fig.6

6/38

Fig.7A

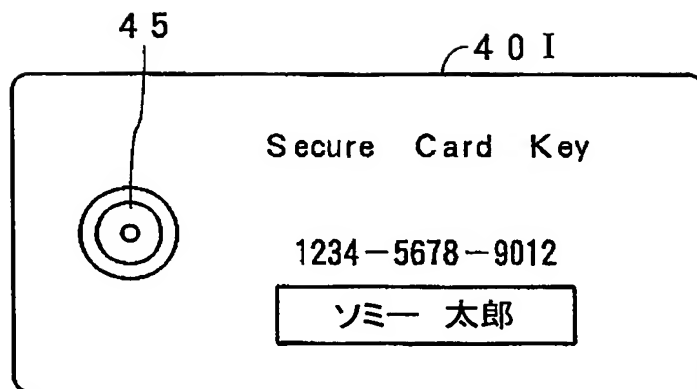
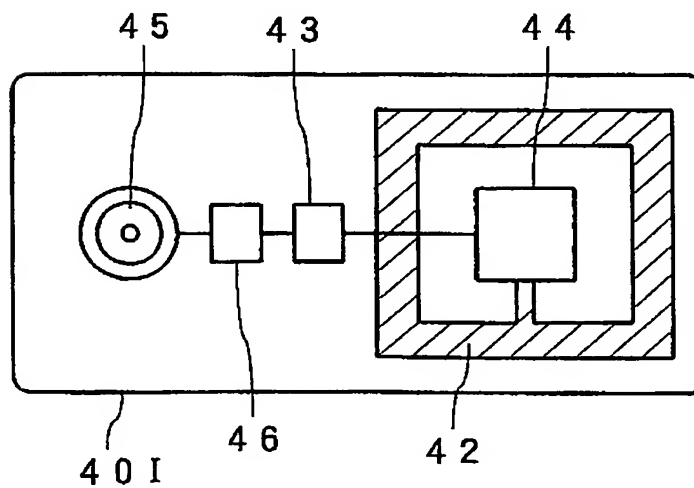


Fig.7B



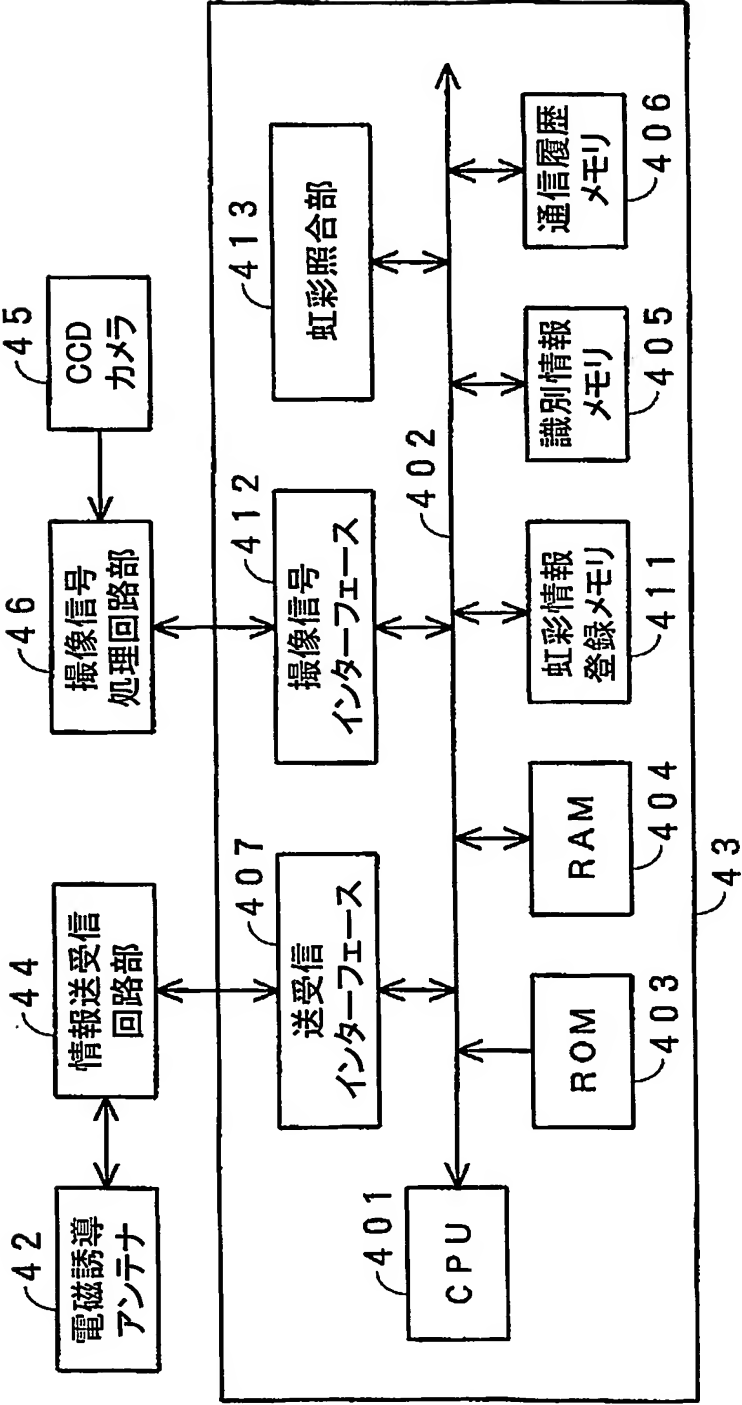


Fig.8

8/38

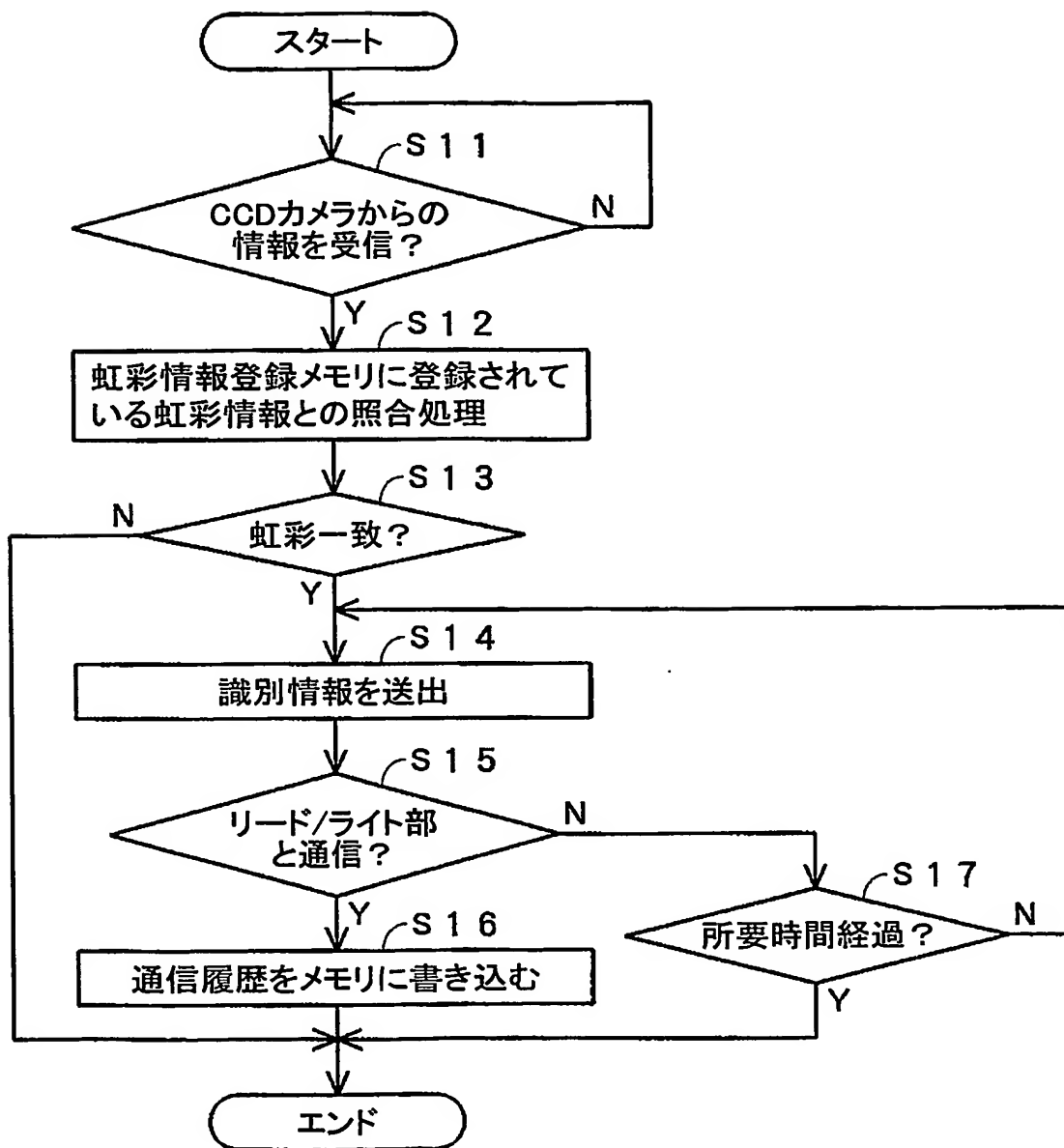


Fig.9

2

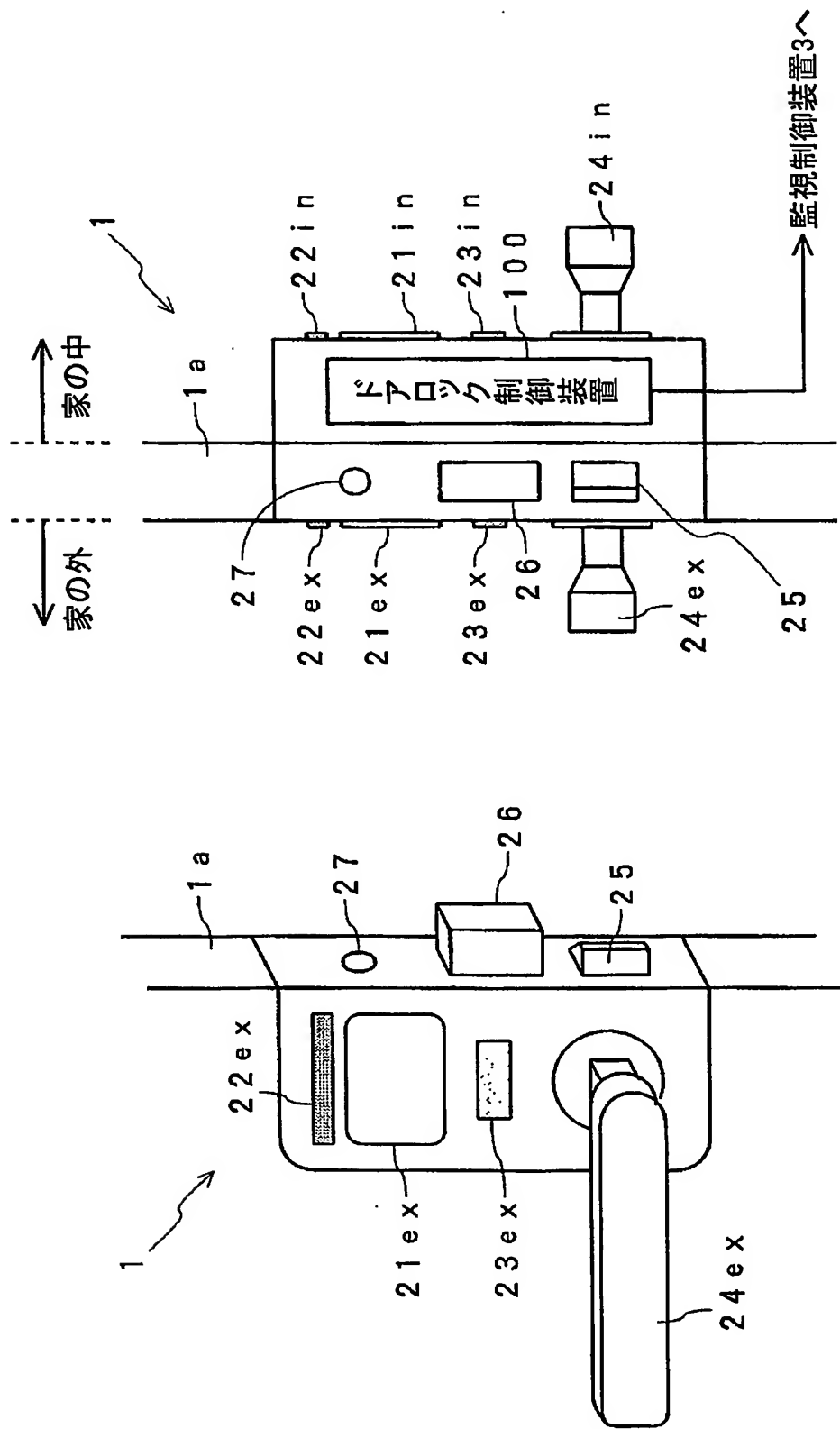


Fig.10B

Fig.10A

10/38

2

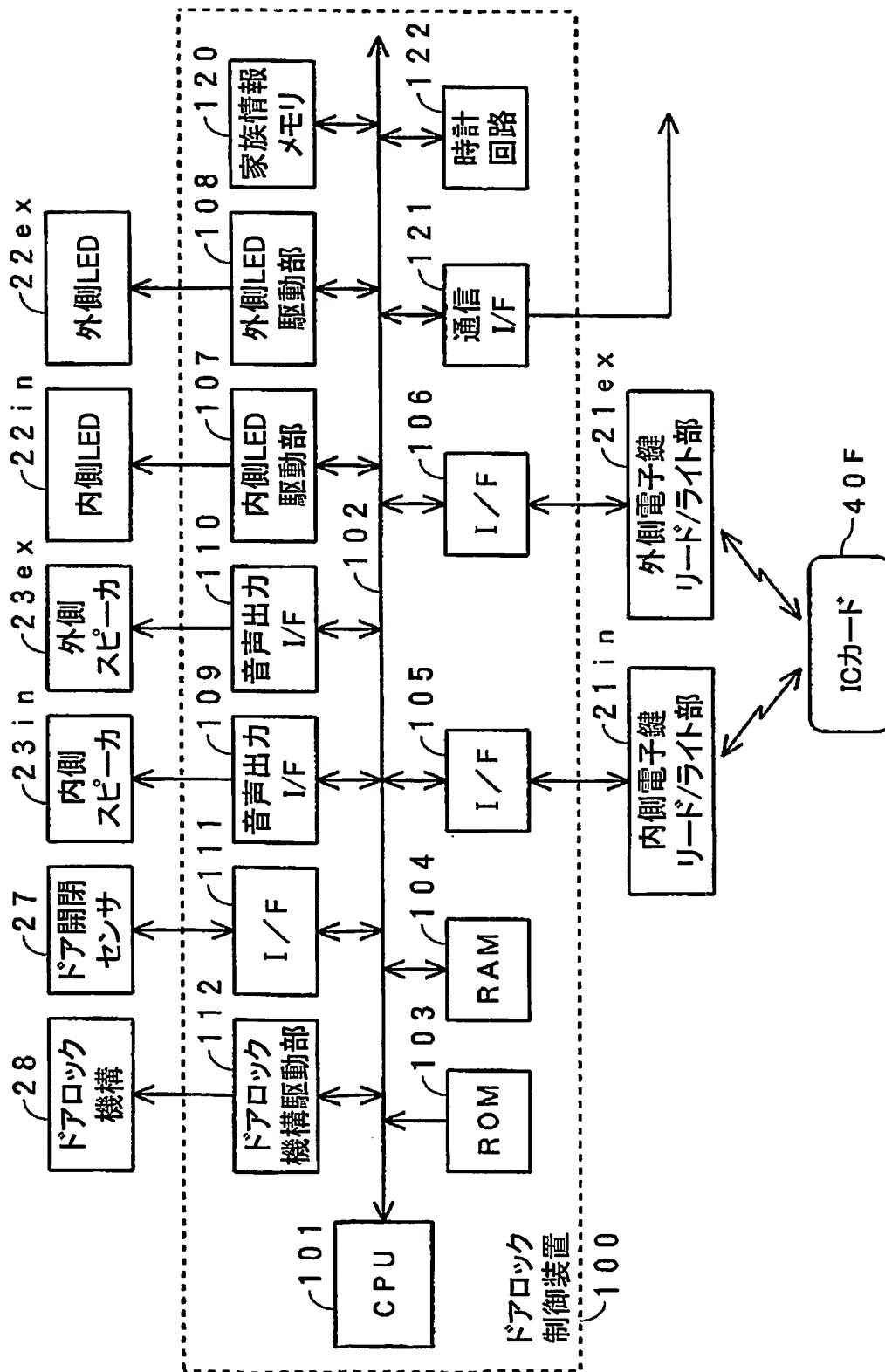


Fig.11

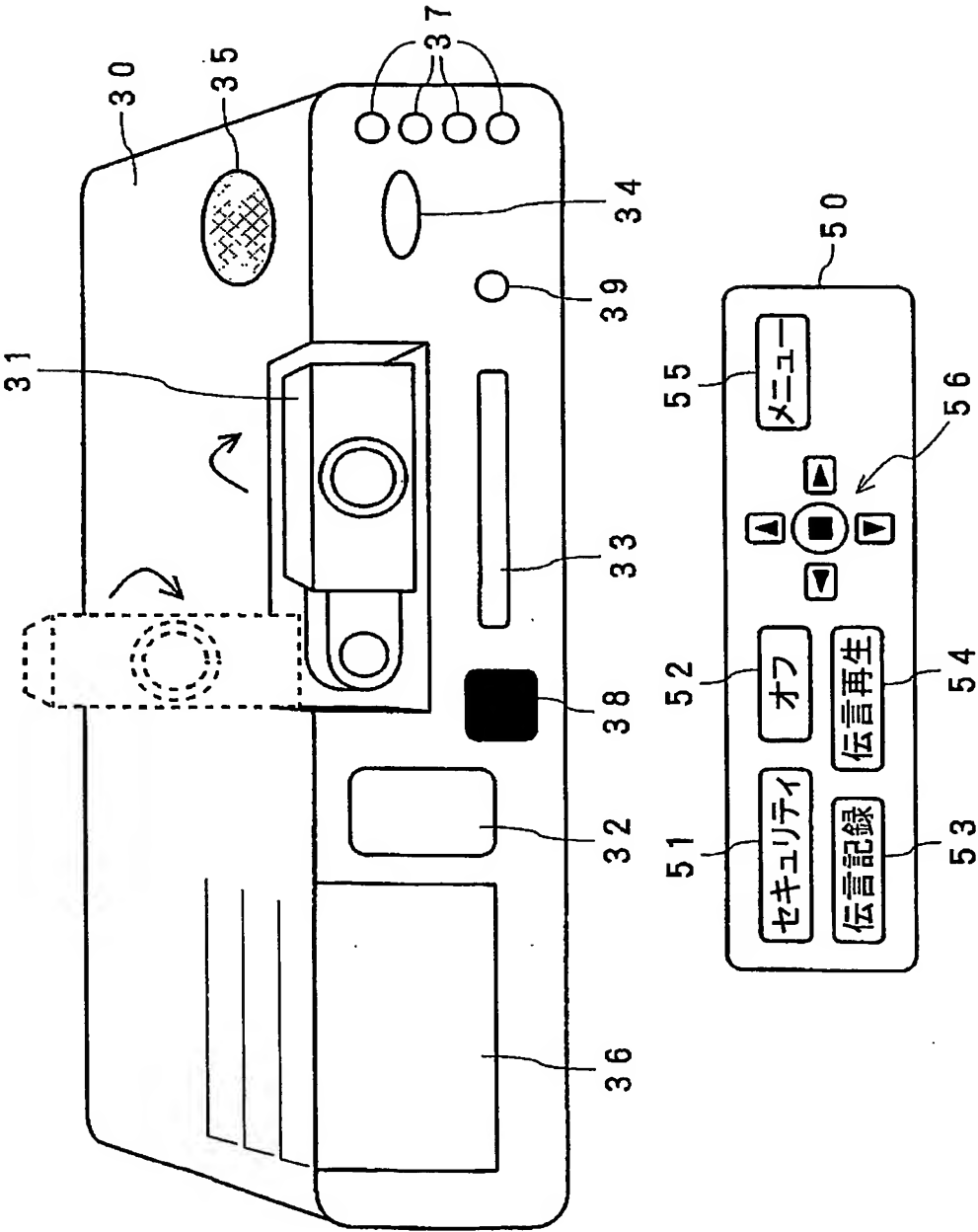


Fig.12

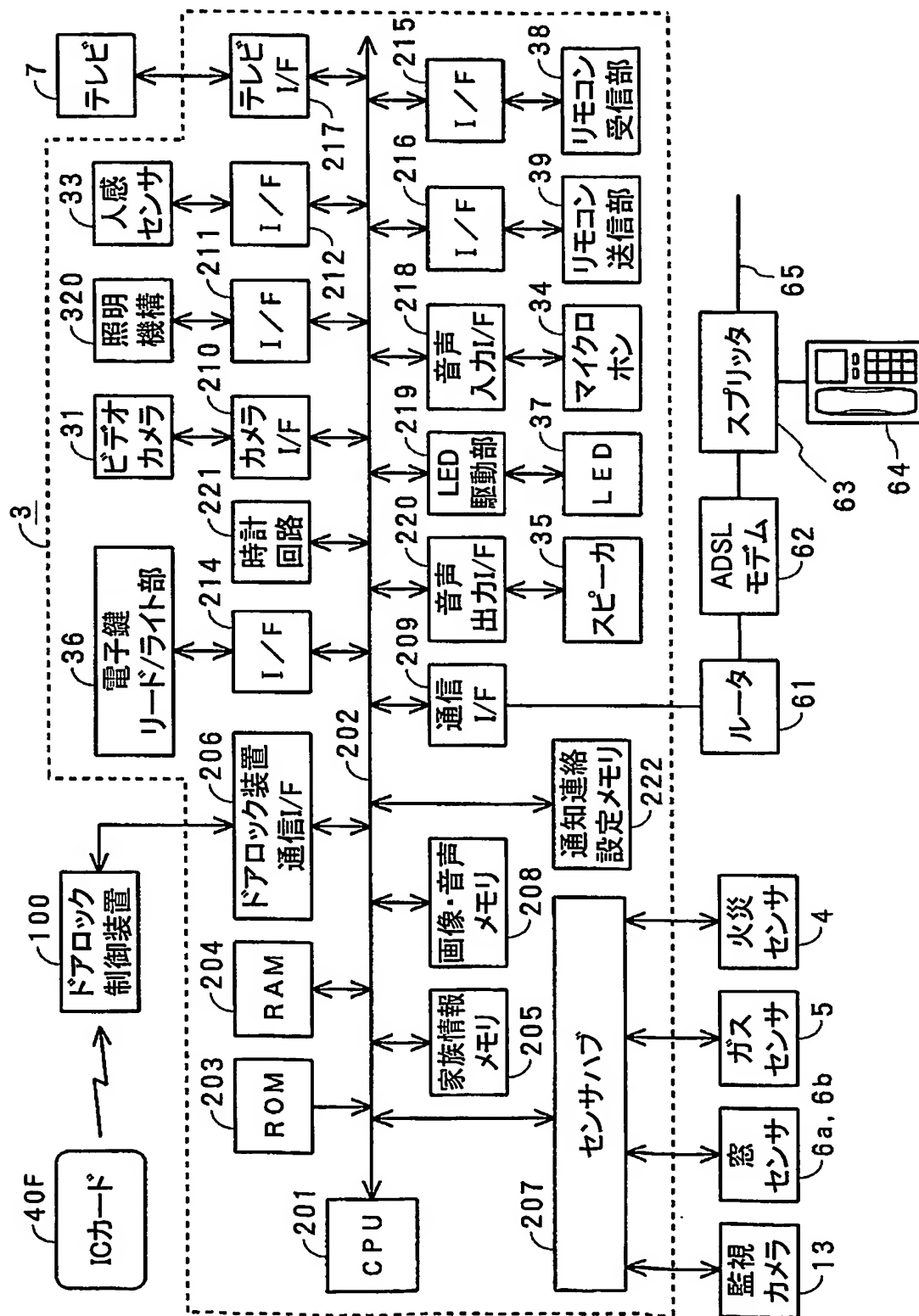


Fig. 13

13/38

	識別情報(ICチップ製造番号) ・本鍵情報 ・バックアップ鍵情報	個人識別情報
	パスワード	
	氏名	個人情報
	住所	
	生年月日	
	年齢	
	続柄	
	登録日	
	銀行口座番号	
	電話番号	
	電子メールアドレス	
	IPアドレス	
	趣味/嗜好情報 ・好きなテレビ番組:ドラマ ・好きな音楽:ジャズ ・好きな映画:SF	
	入退出履歴情報	
	電子鍵登録・紛失履歴情報	

Fig.14

14/38

セキュリティレベル	父親	母親	子供	
D	○	○	○	○ : 在宅
D	○	○	×	×
D	○	×	○	×
D	○	×	×	×
C	×	○	○	×
C	×	○	×	×
B	×	×	○	×
A	×	×	×	×

Fig.15

セキュリティレベル	窓・ドア監視	火災・ガス監視	カメラ監視
A	○	○	○
B	○	○	×
C	×	○	×
D	×	×	×

Fig.16

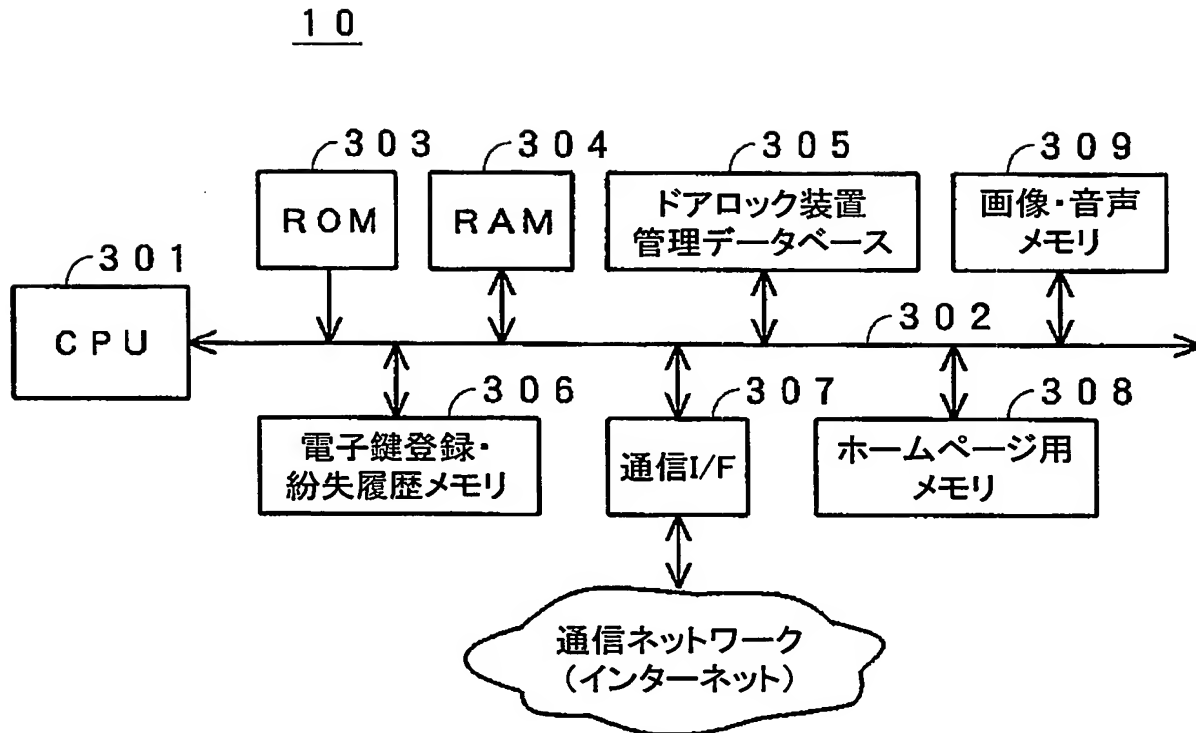


Fig.17

16/38

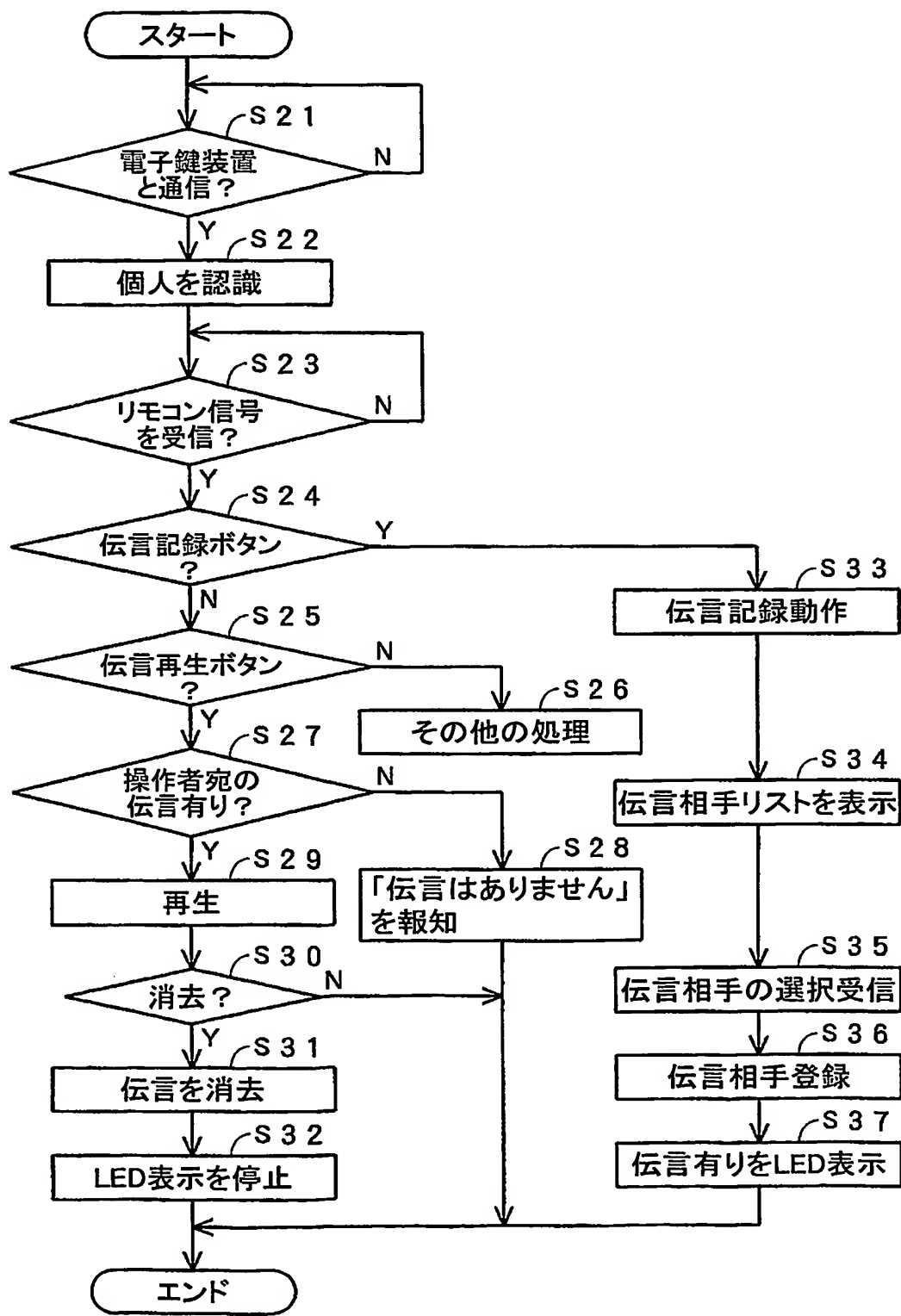


Fig.18

17/38

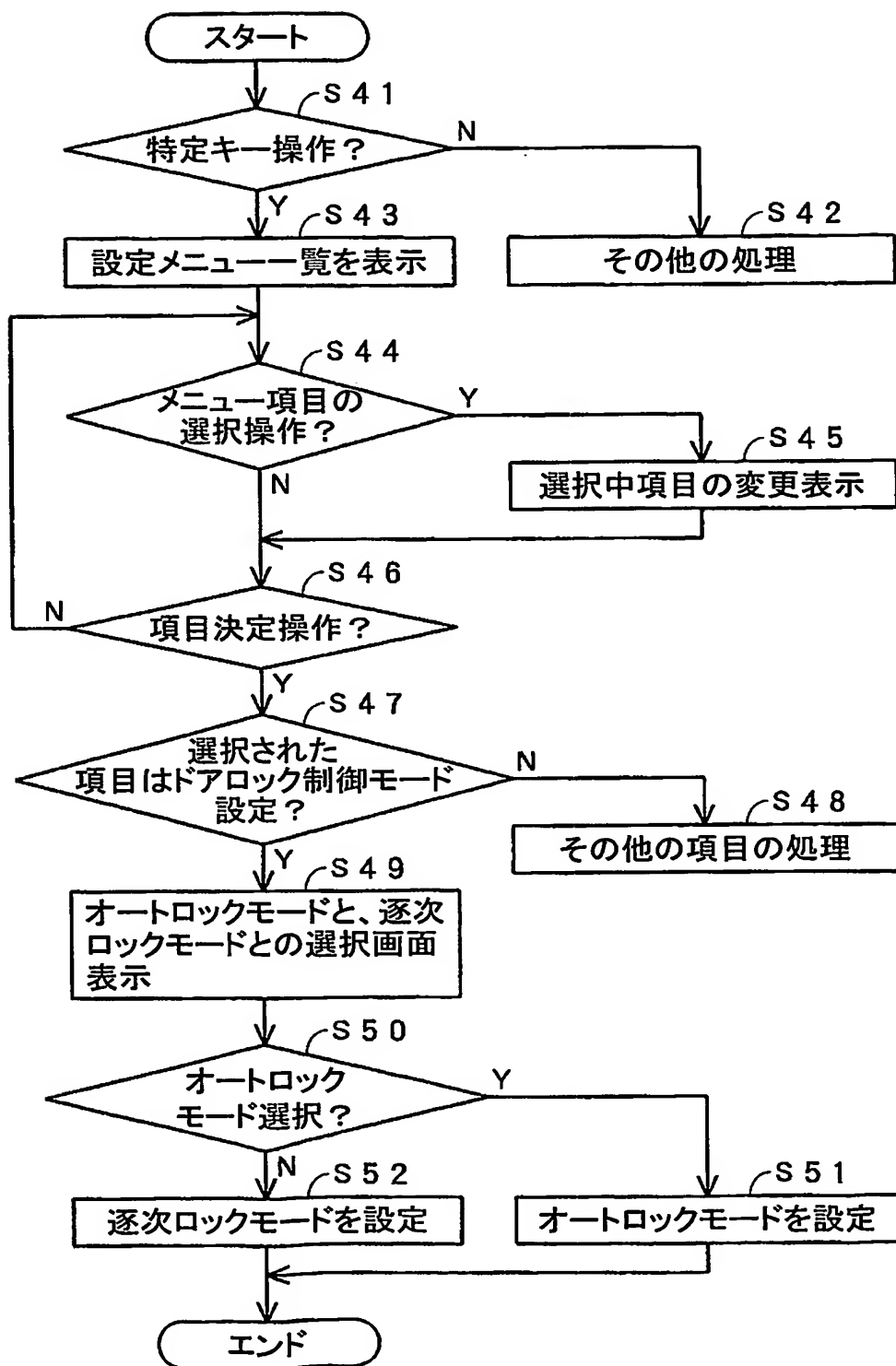


Fig.19

18/38

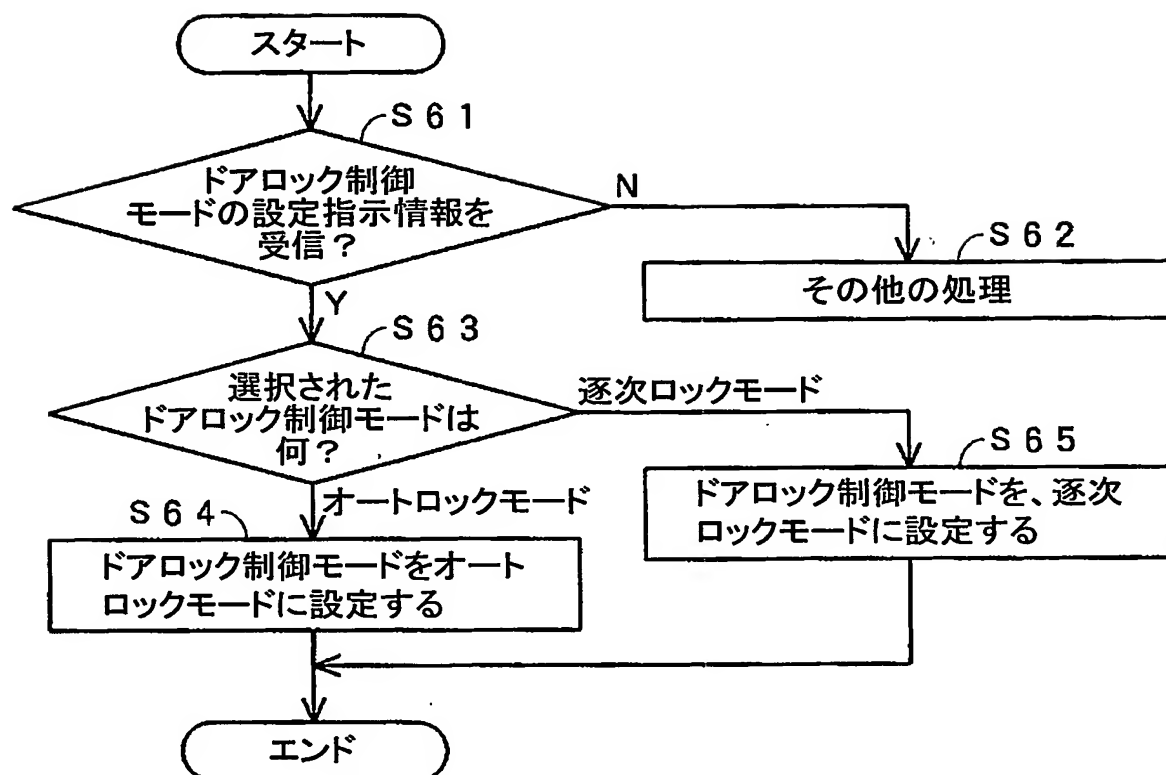


Fig.20

19/38

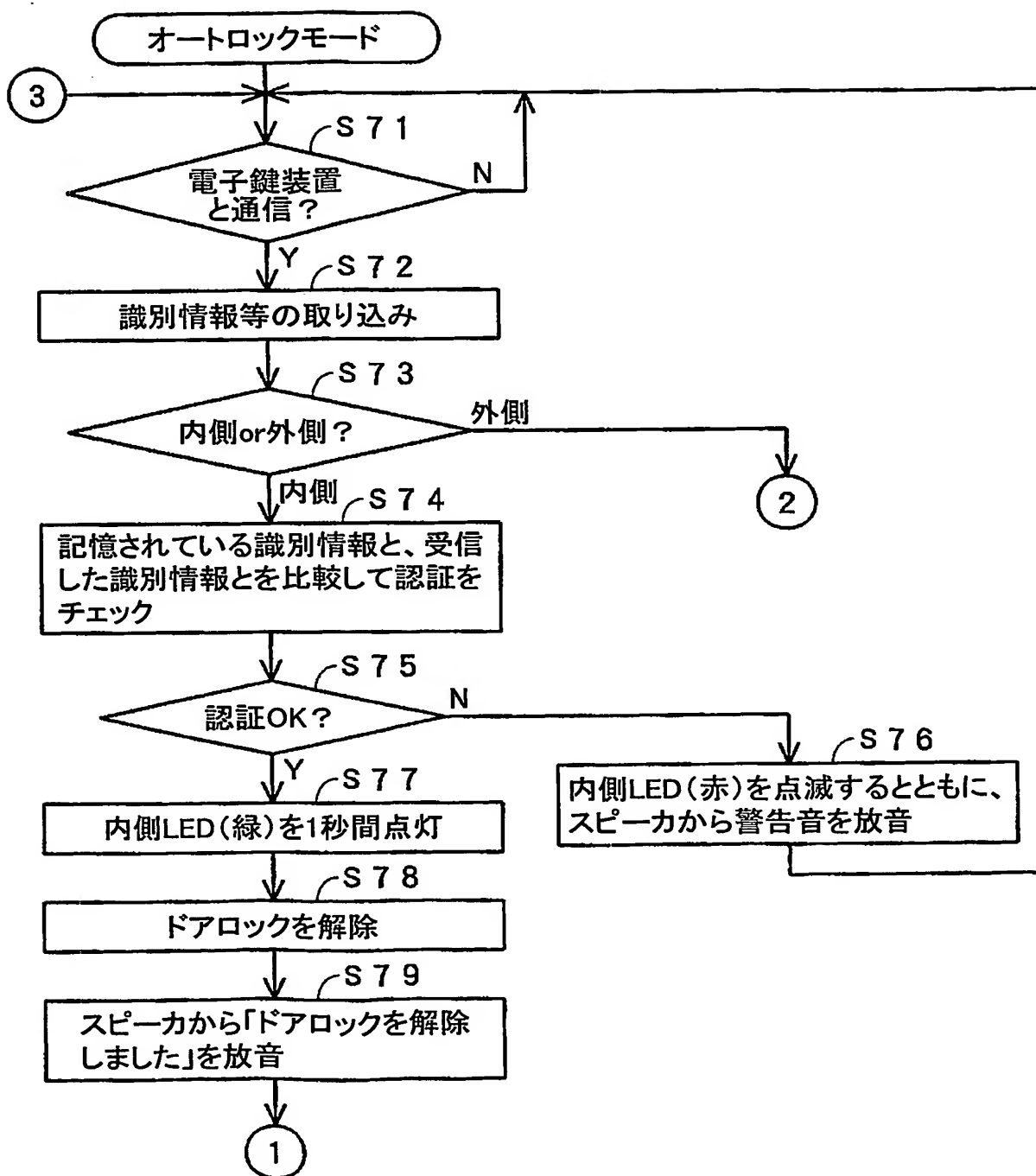


Fig.21

20/38

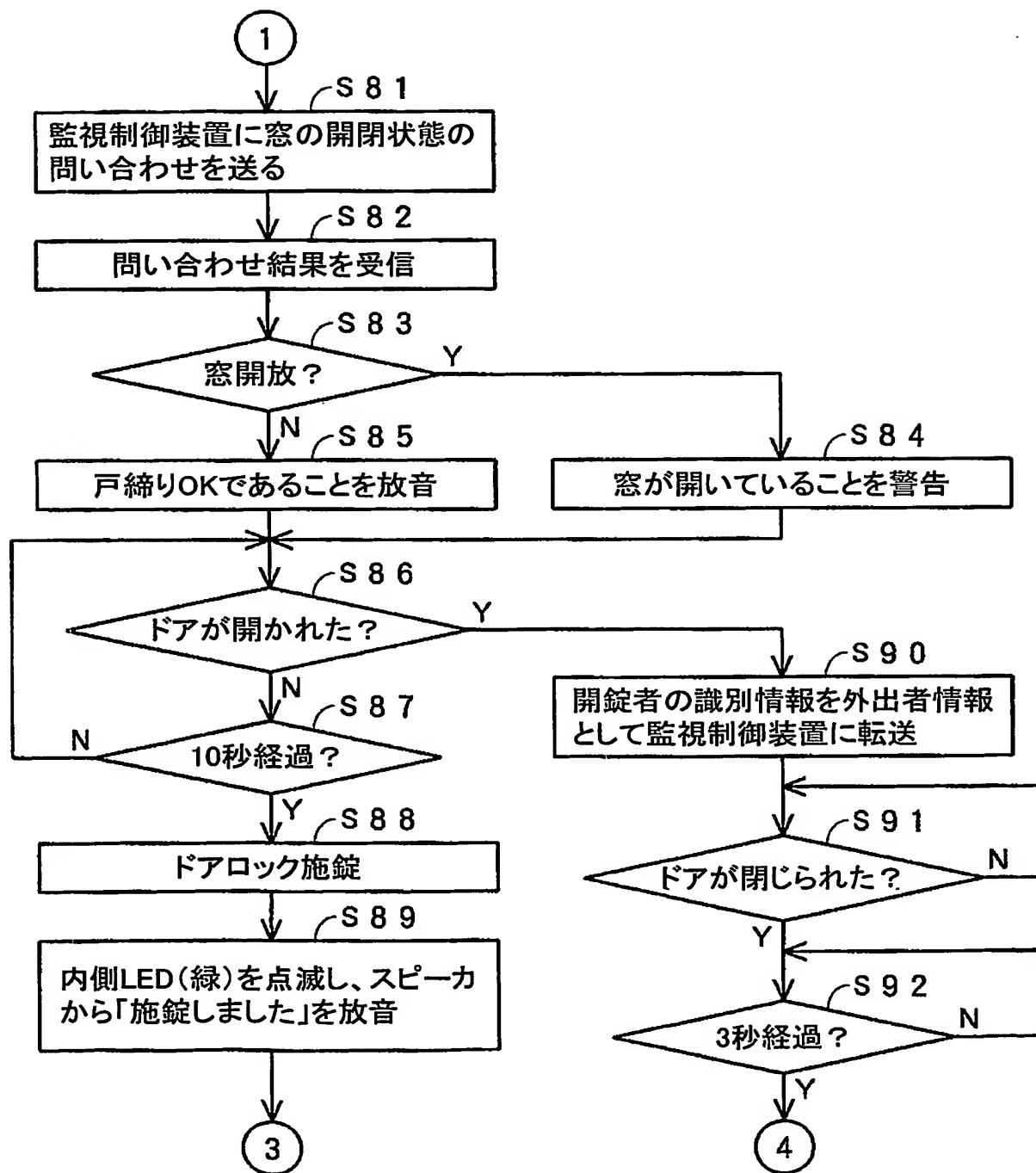


Fig.22

21/38

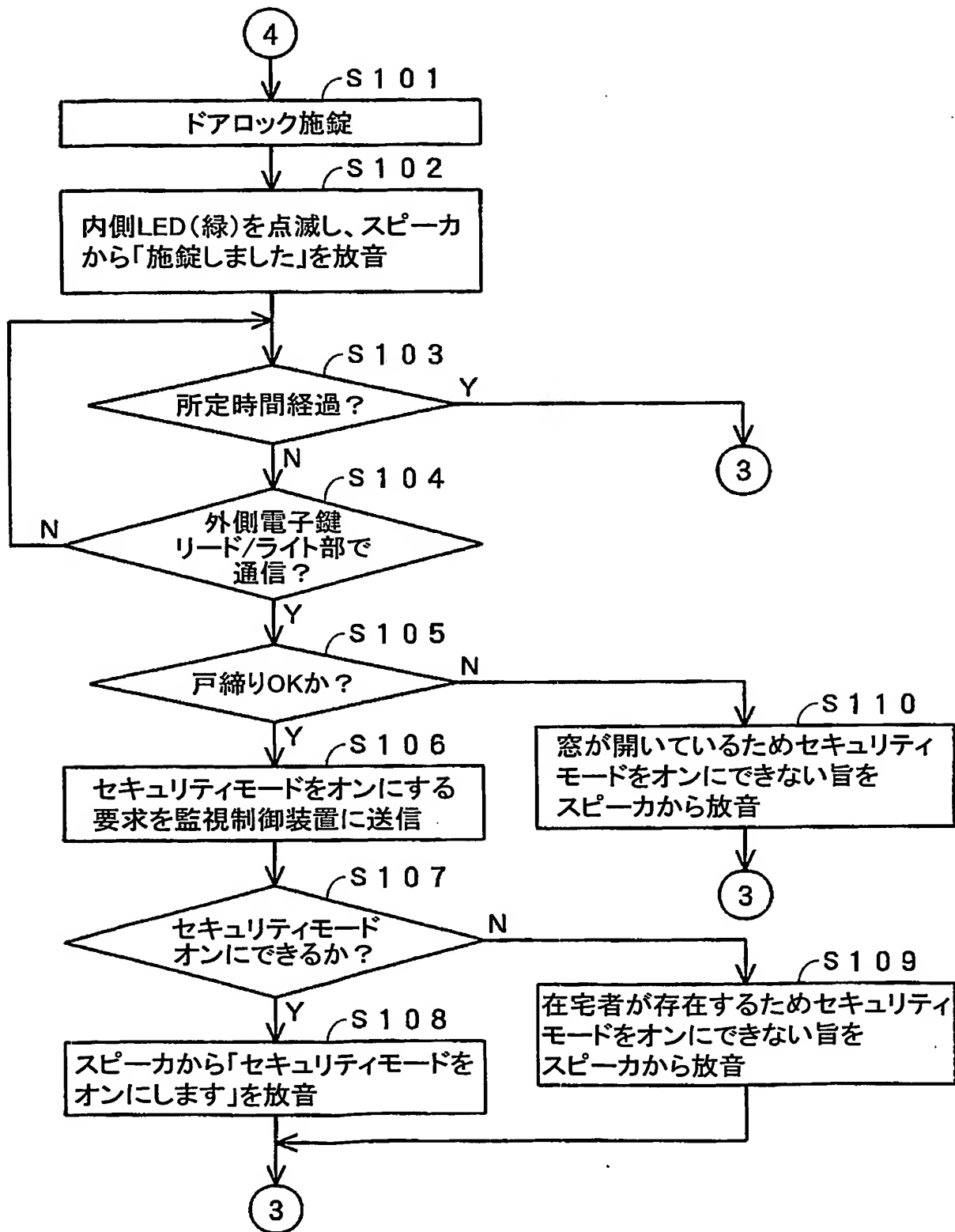


Fig.23

22/38

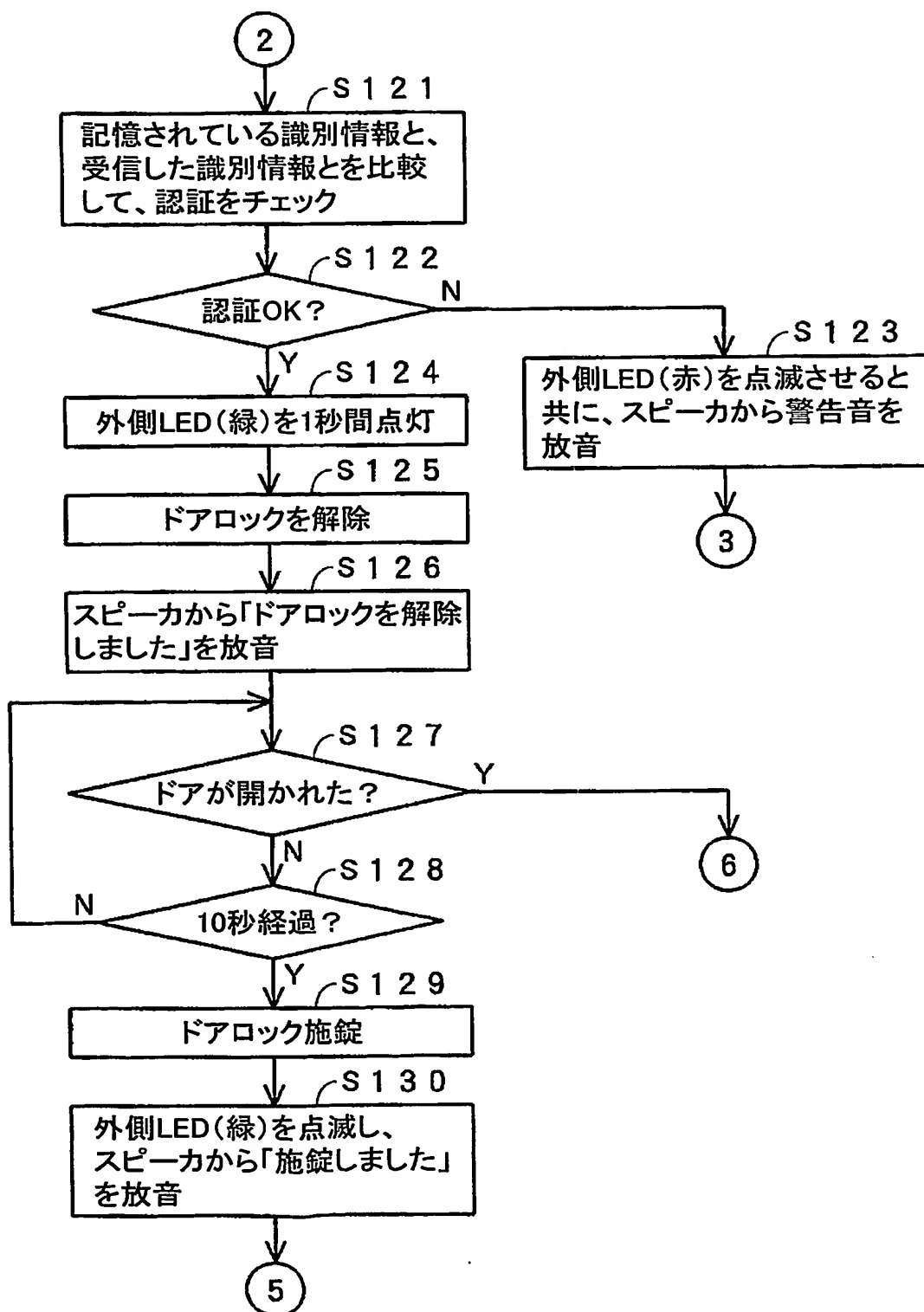


Fig.24

23/38

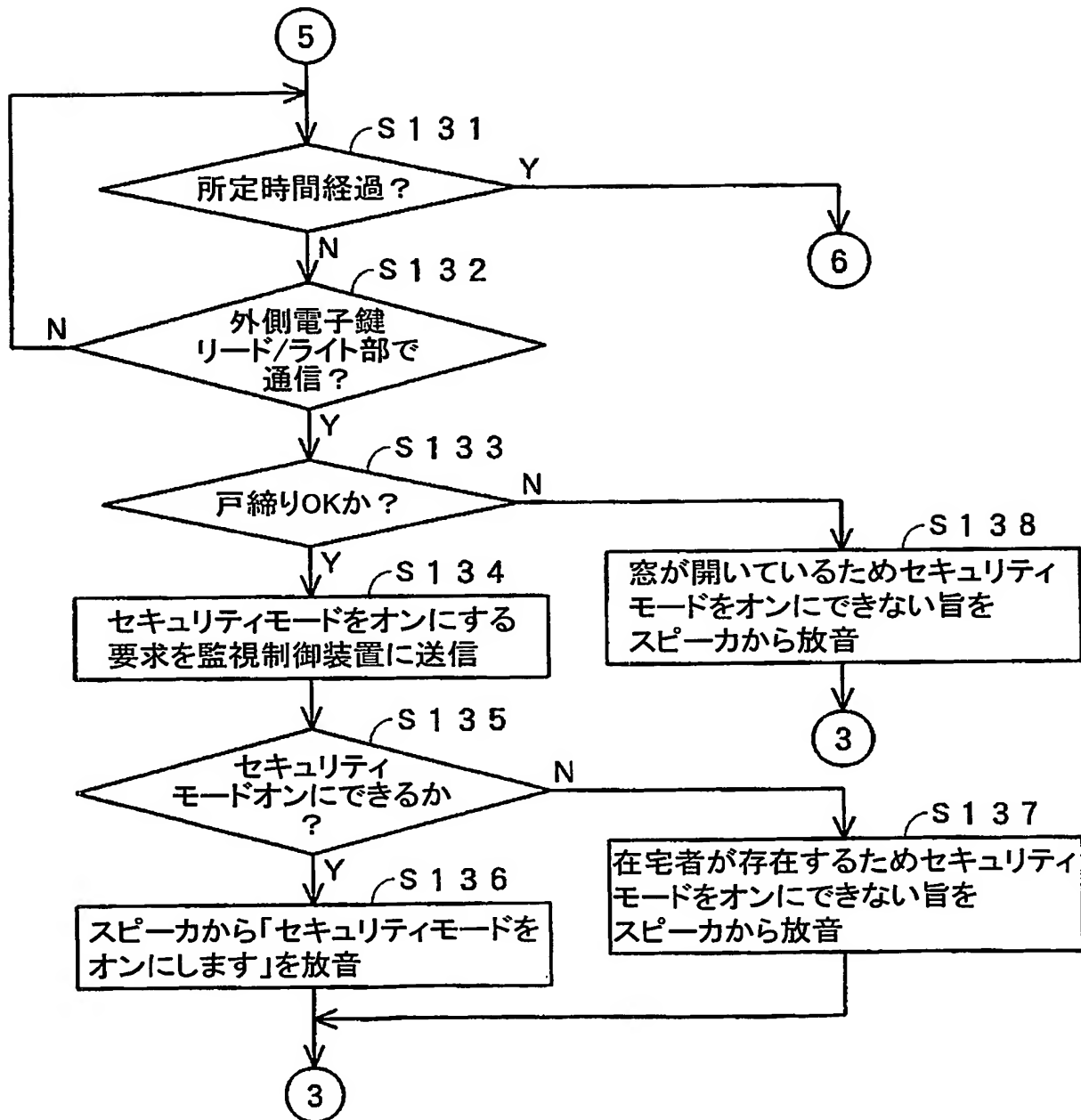


Fig.25

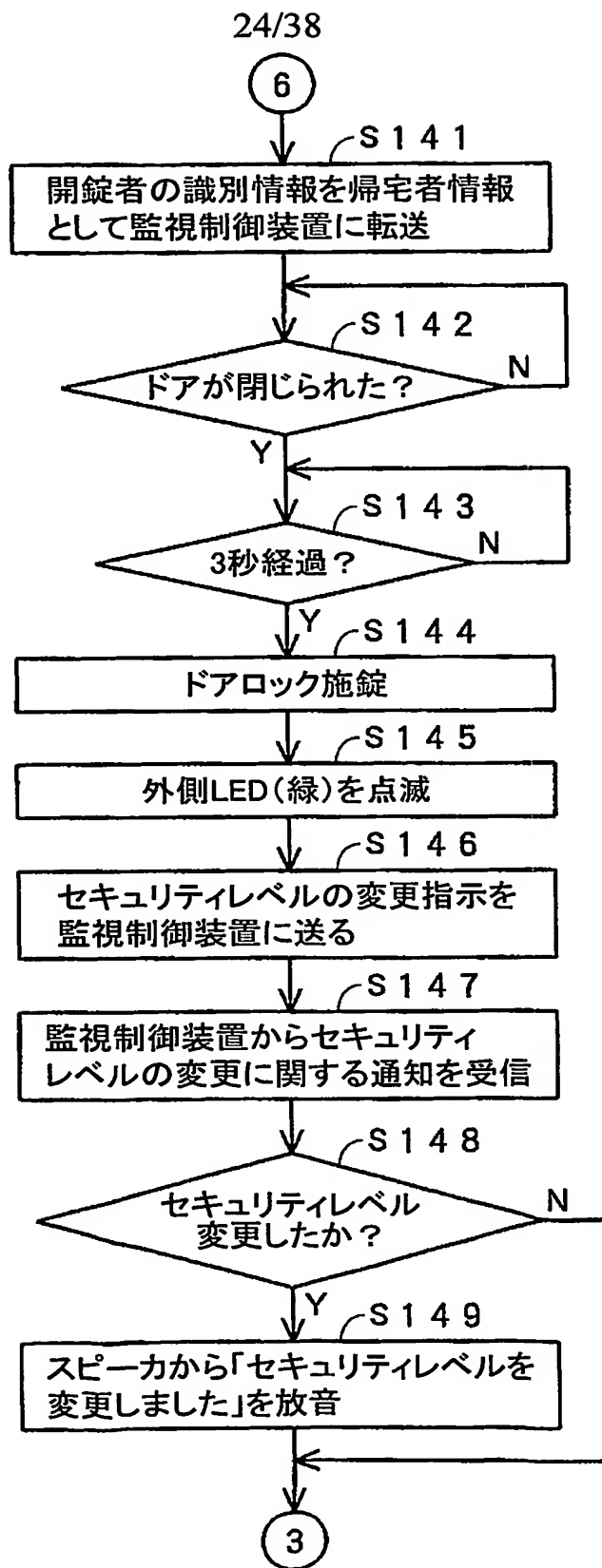


Fig.26

25/38

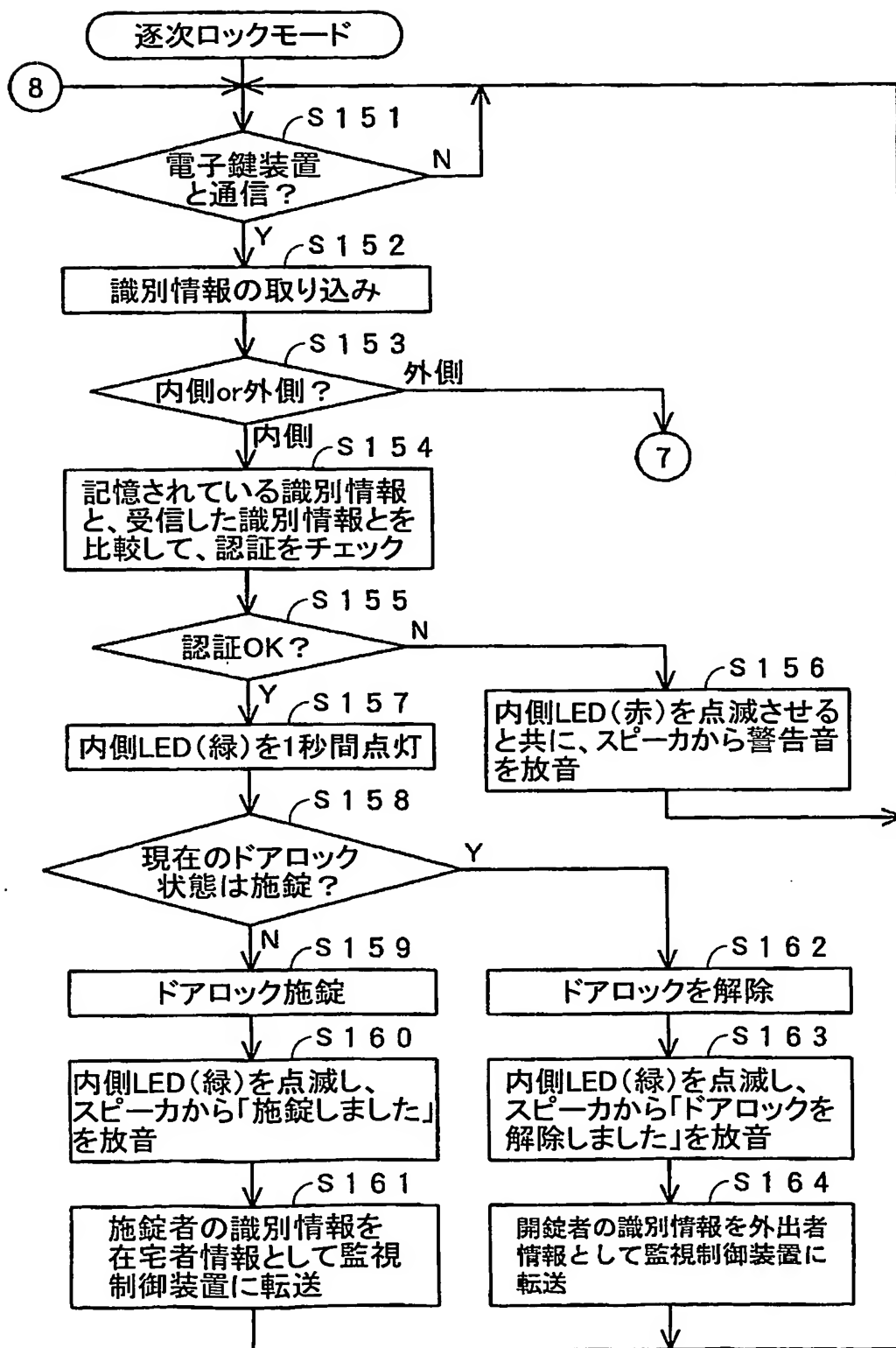


Fig.27

26/38

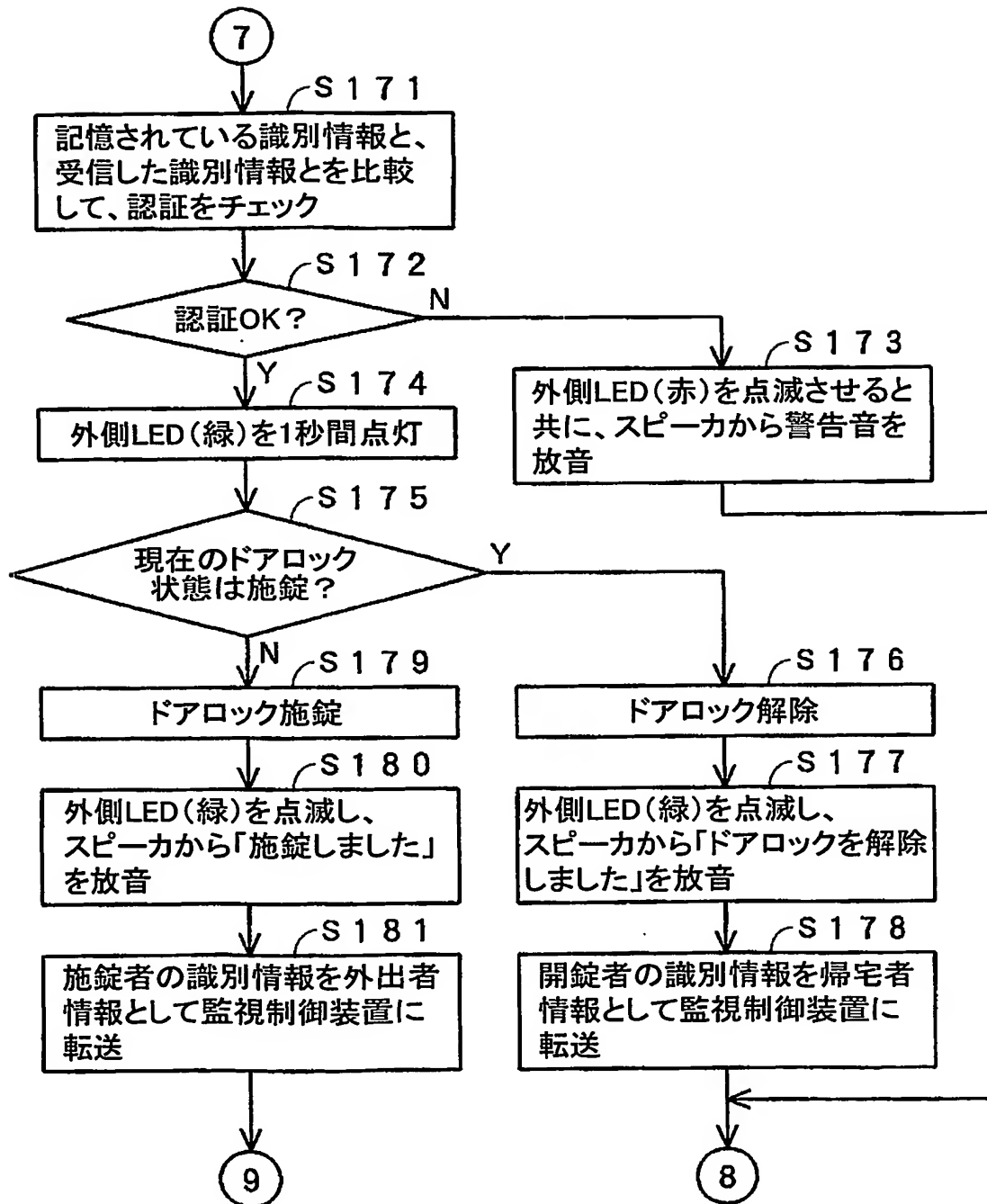


Fig.28

27/38

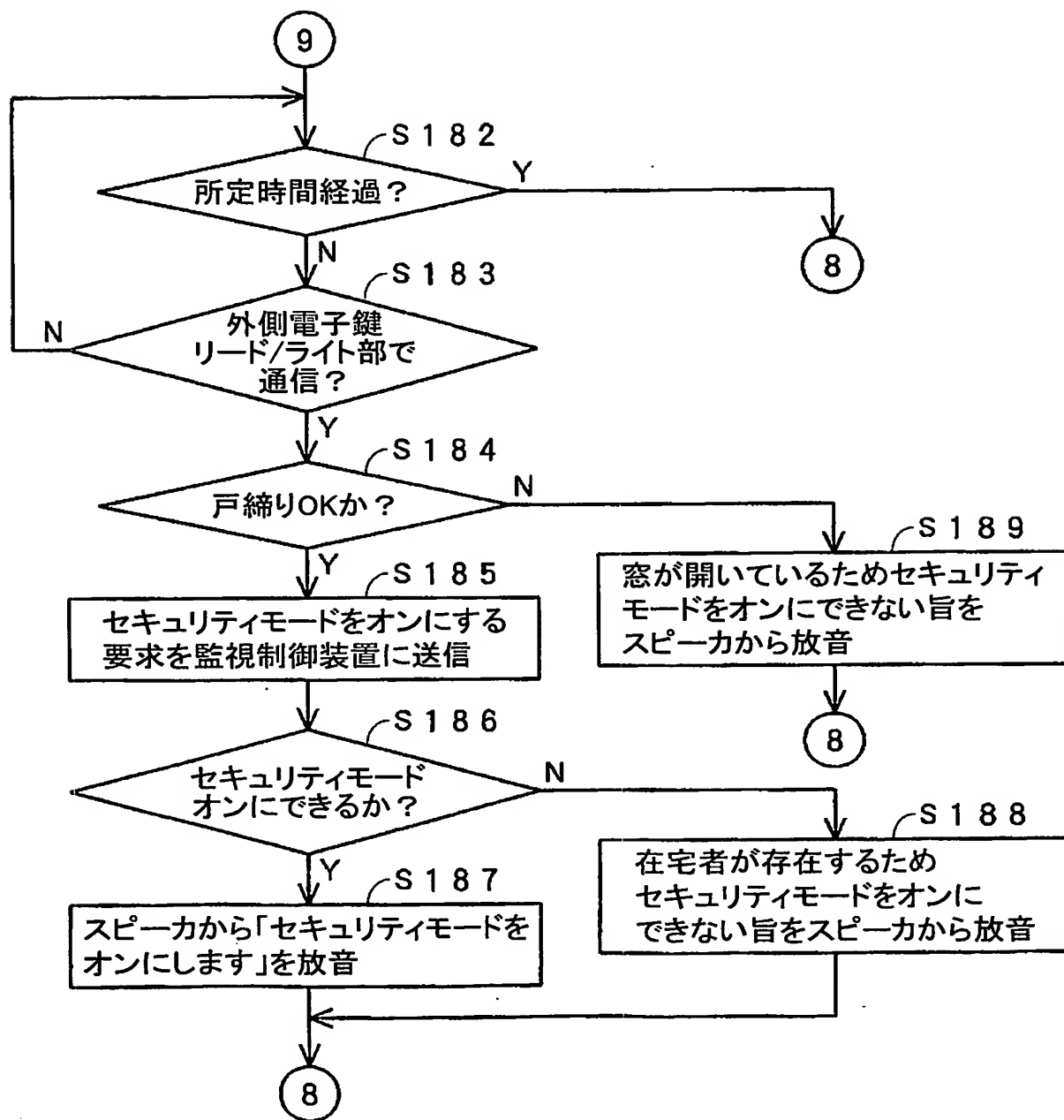


Fig.29

28/38

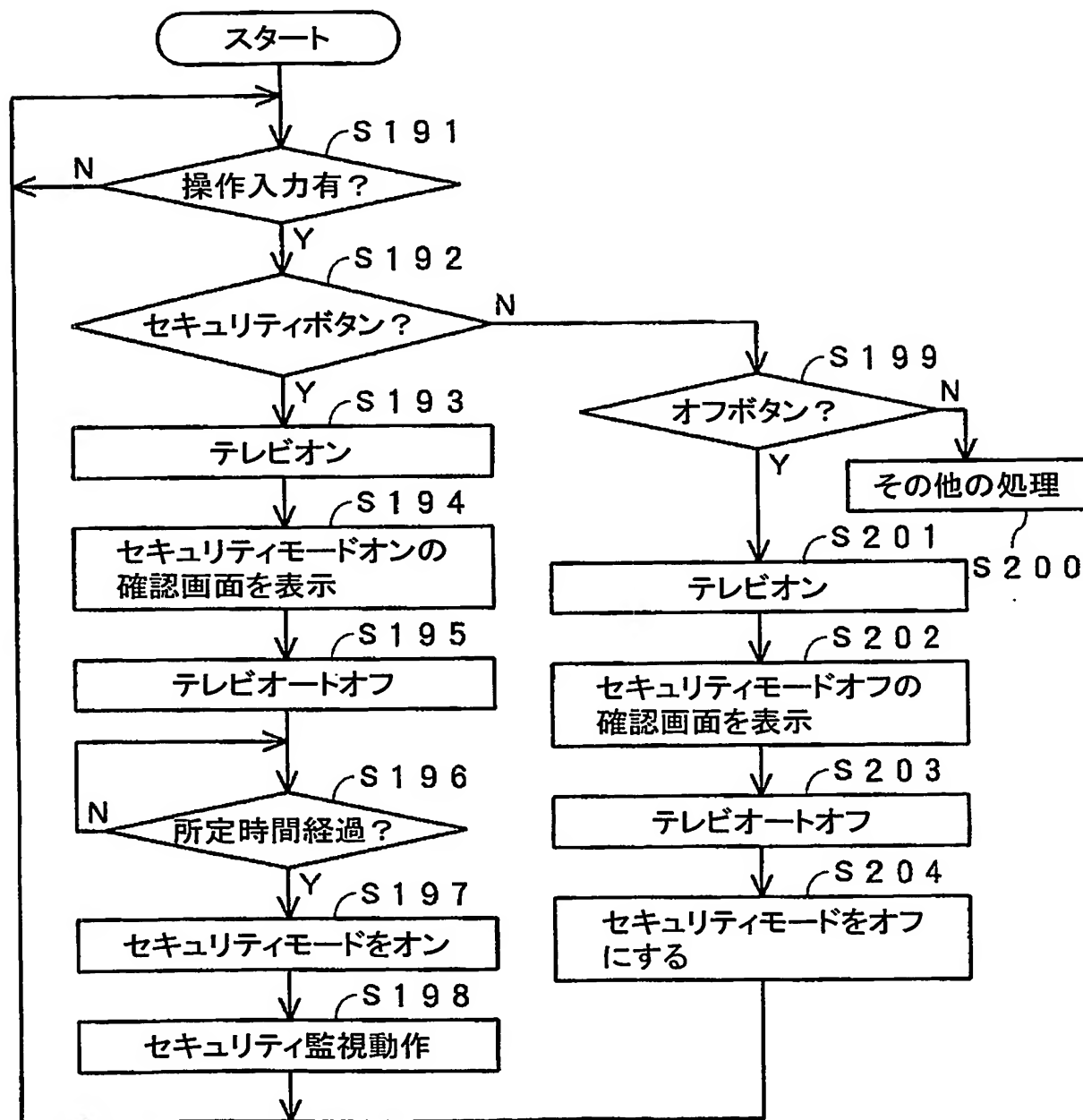


Fig.30

29/38

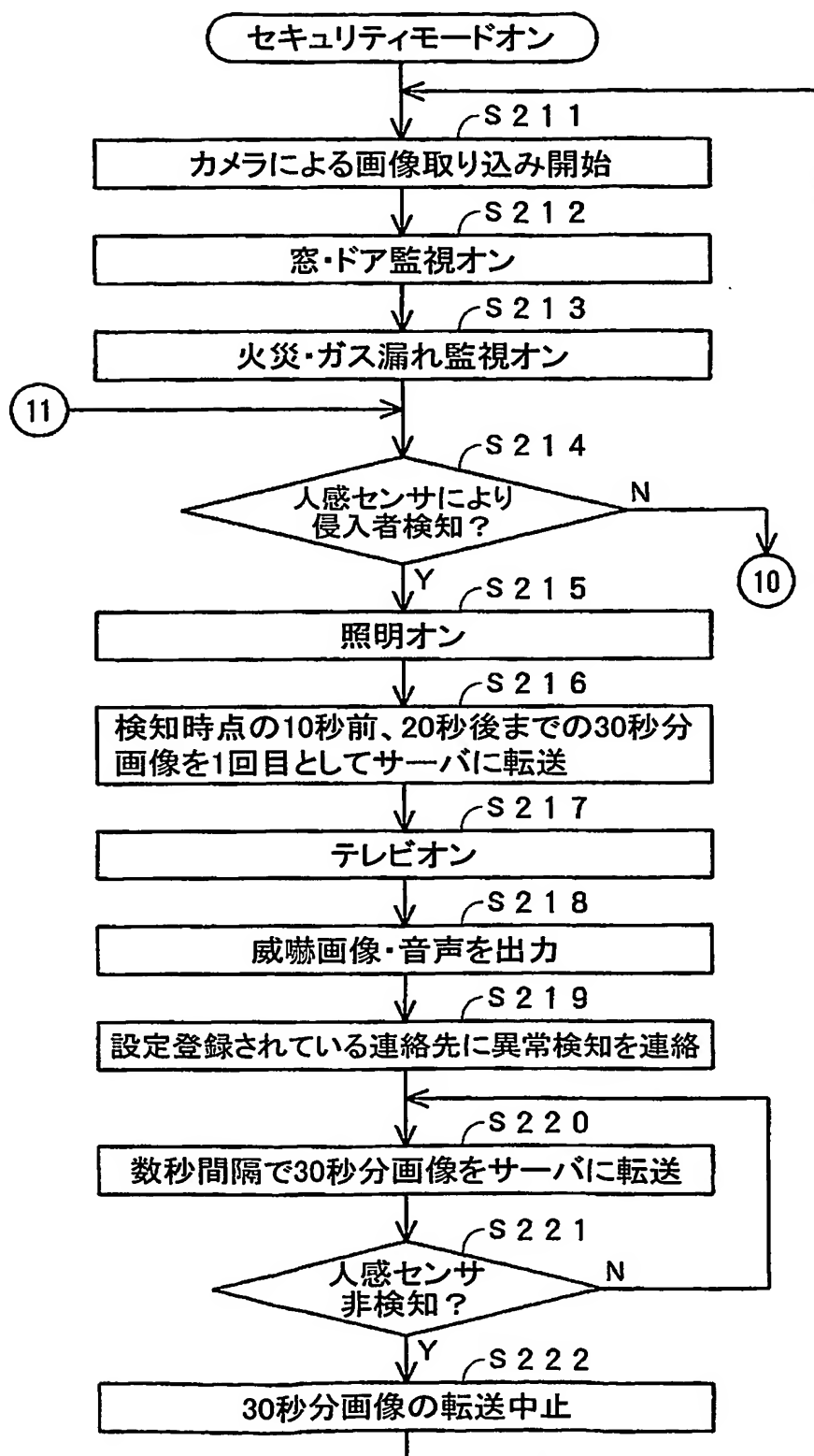


Fig.31

30/38

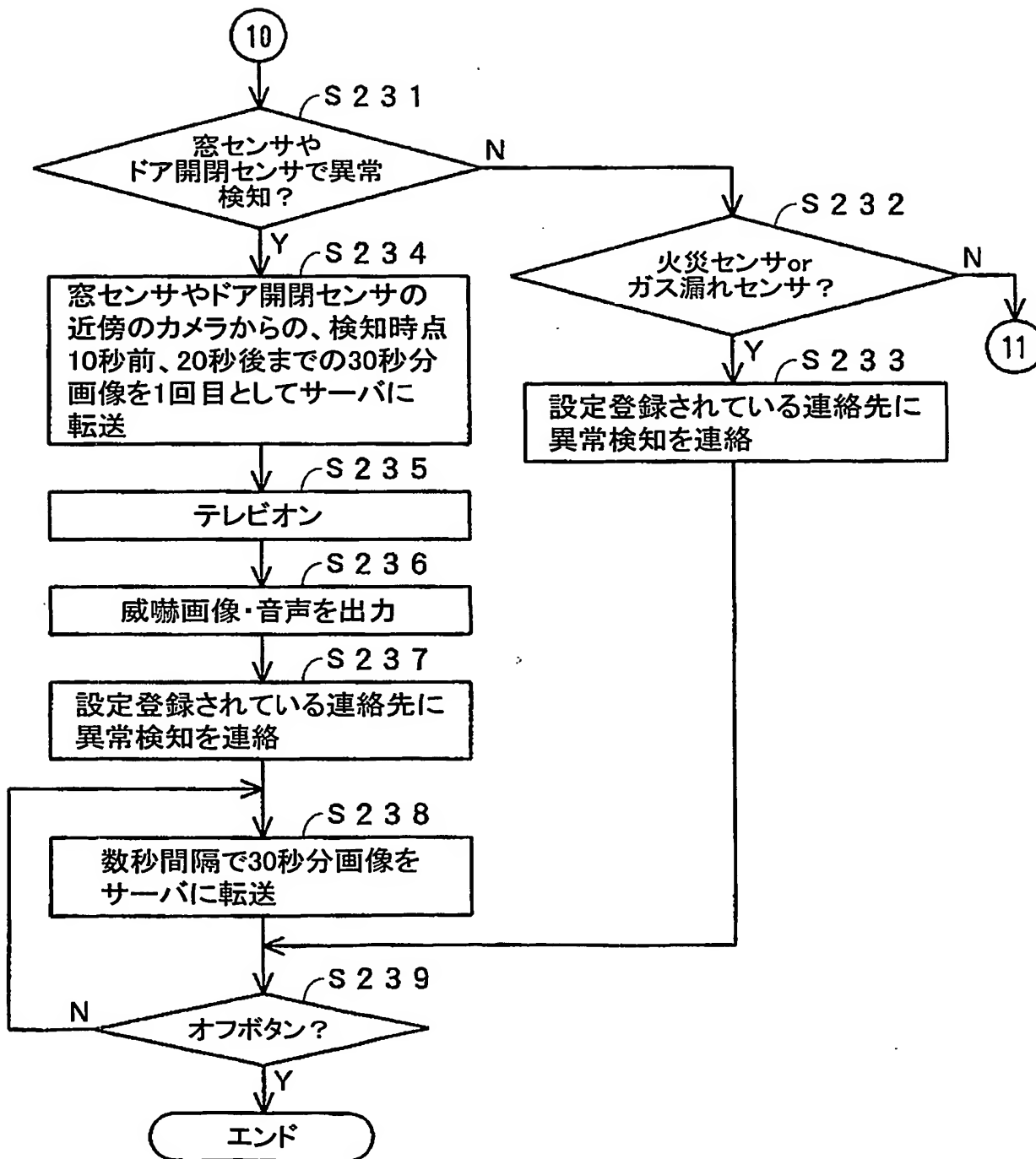


Fig.32

31/38

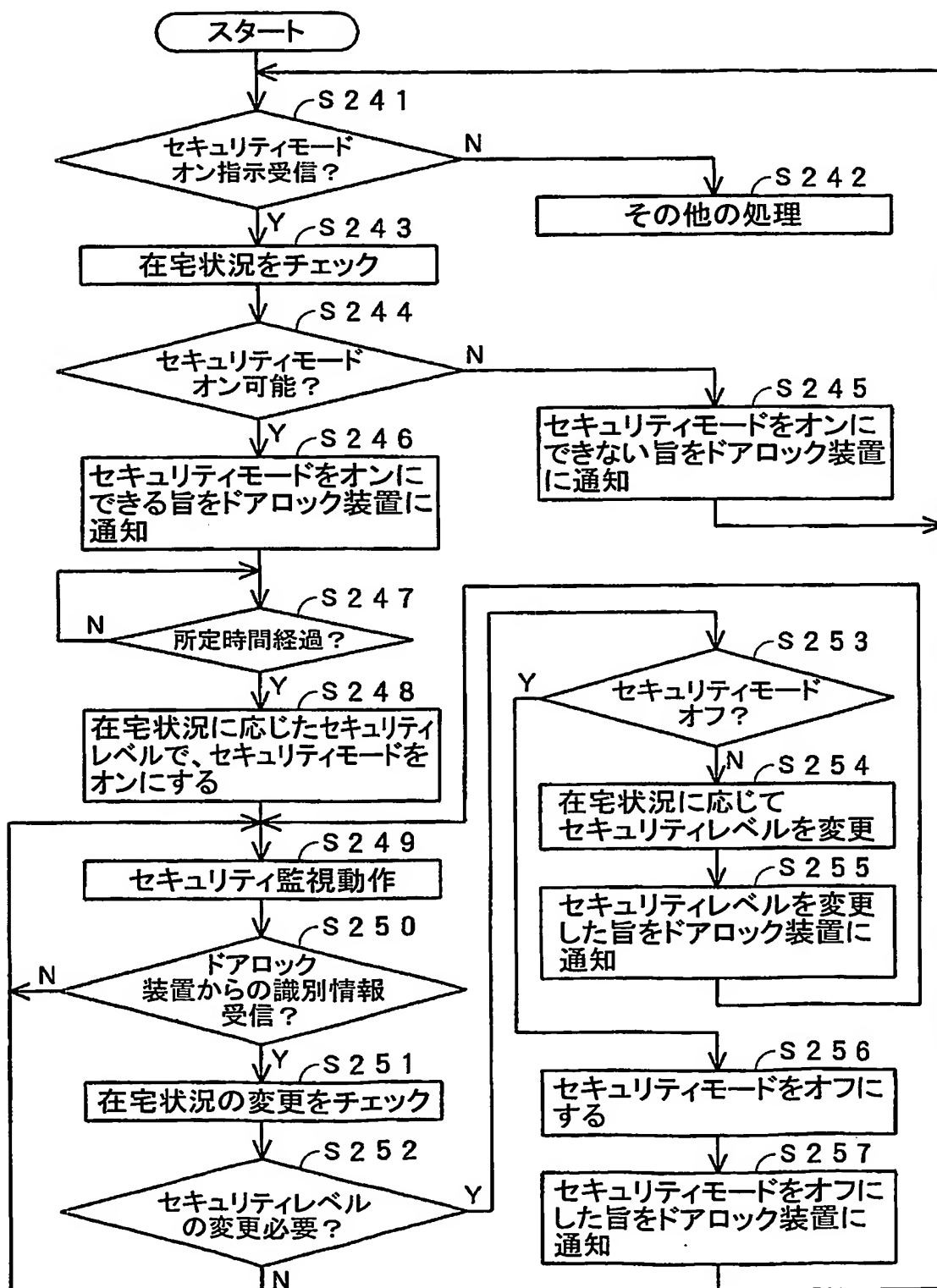


Fig.33

32/38

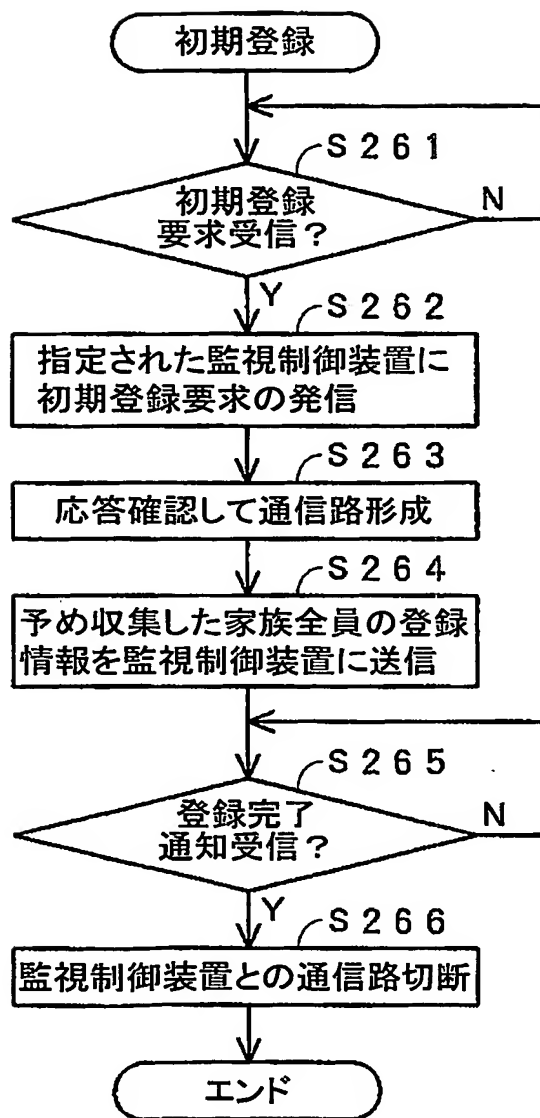


Fig.34

33/38

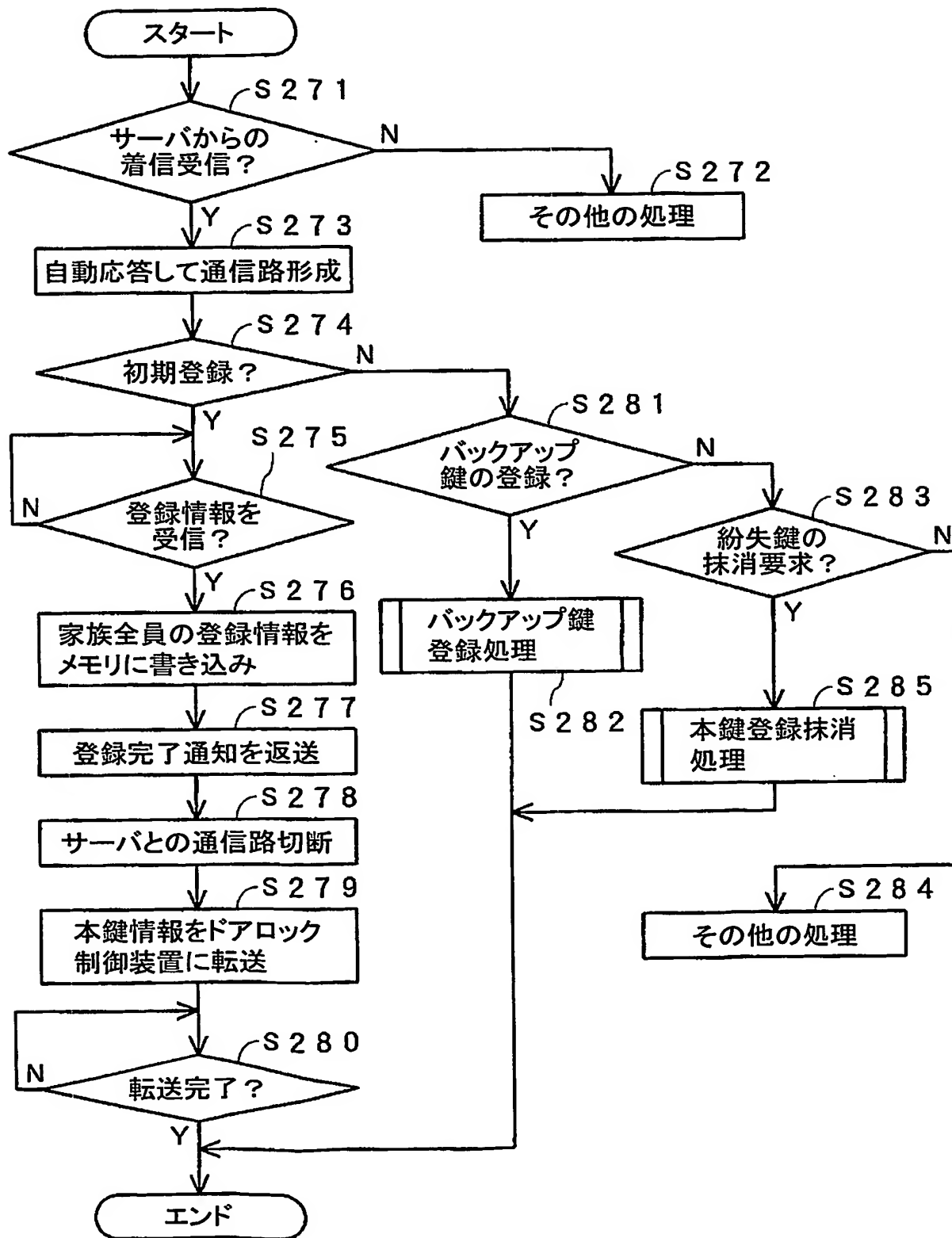


Fig.35

34/38

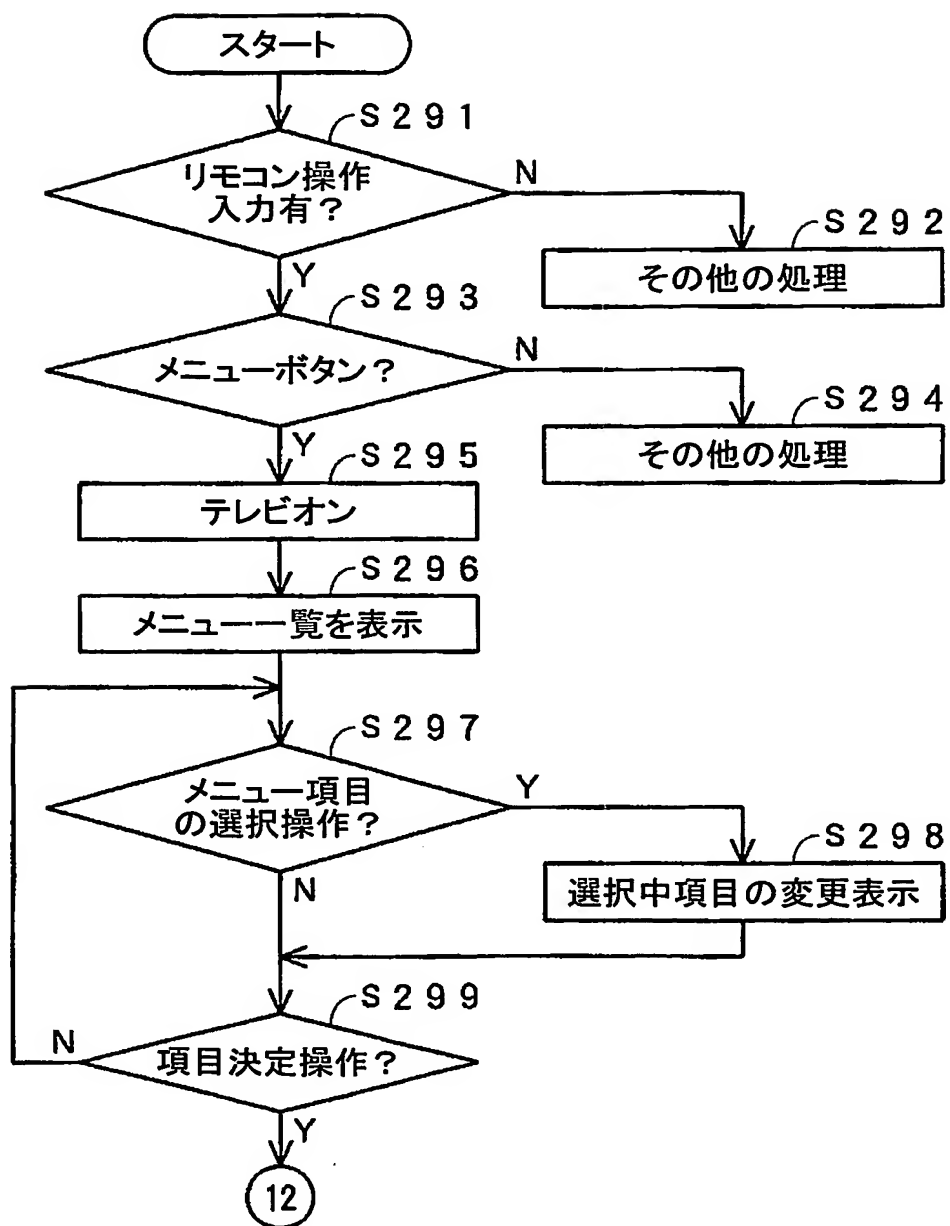


Fig.36

35/38

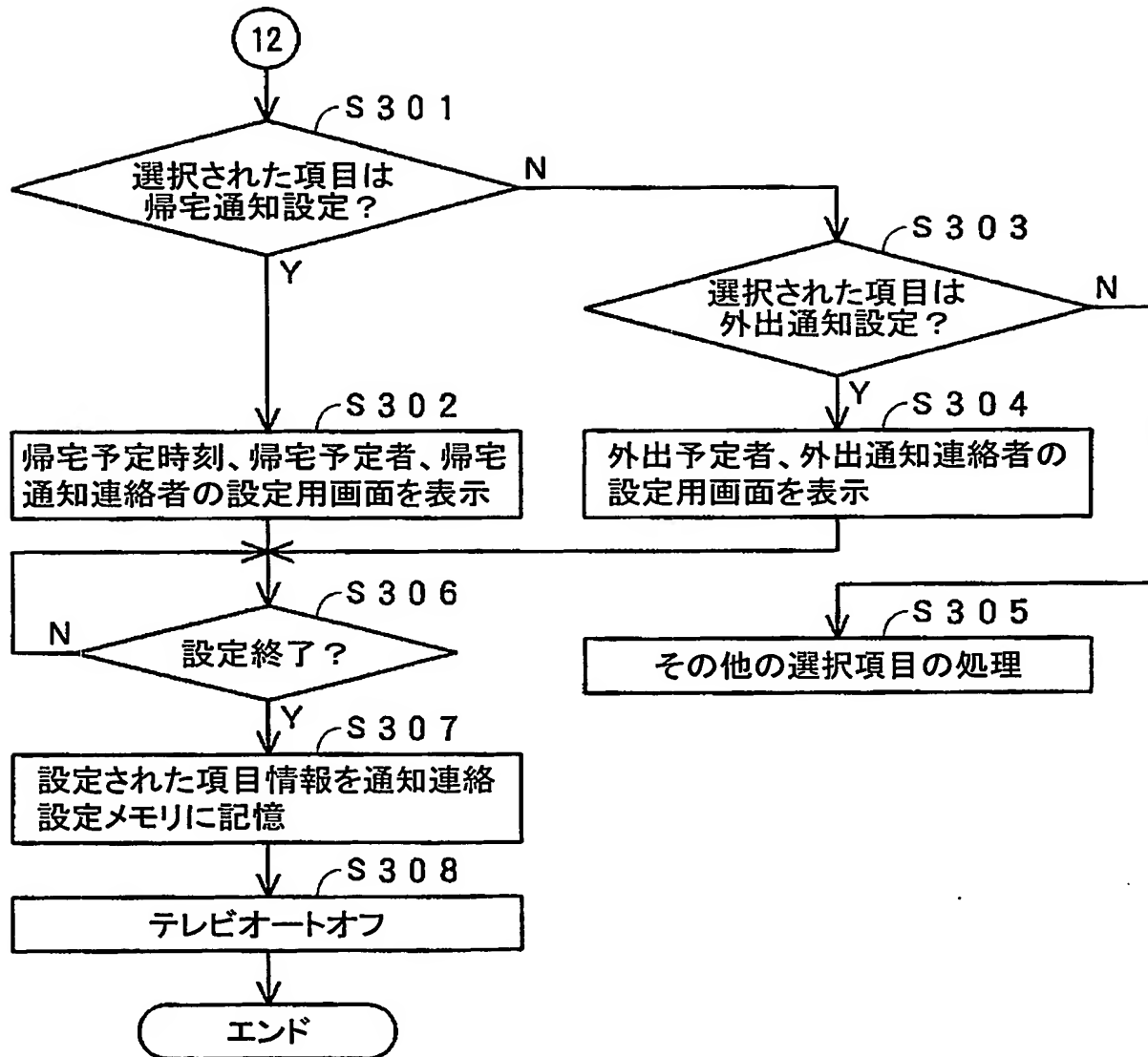


Fig.37

36/38

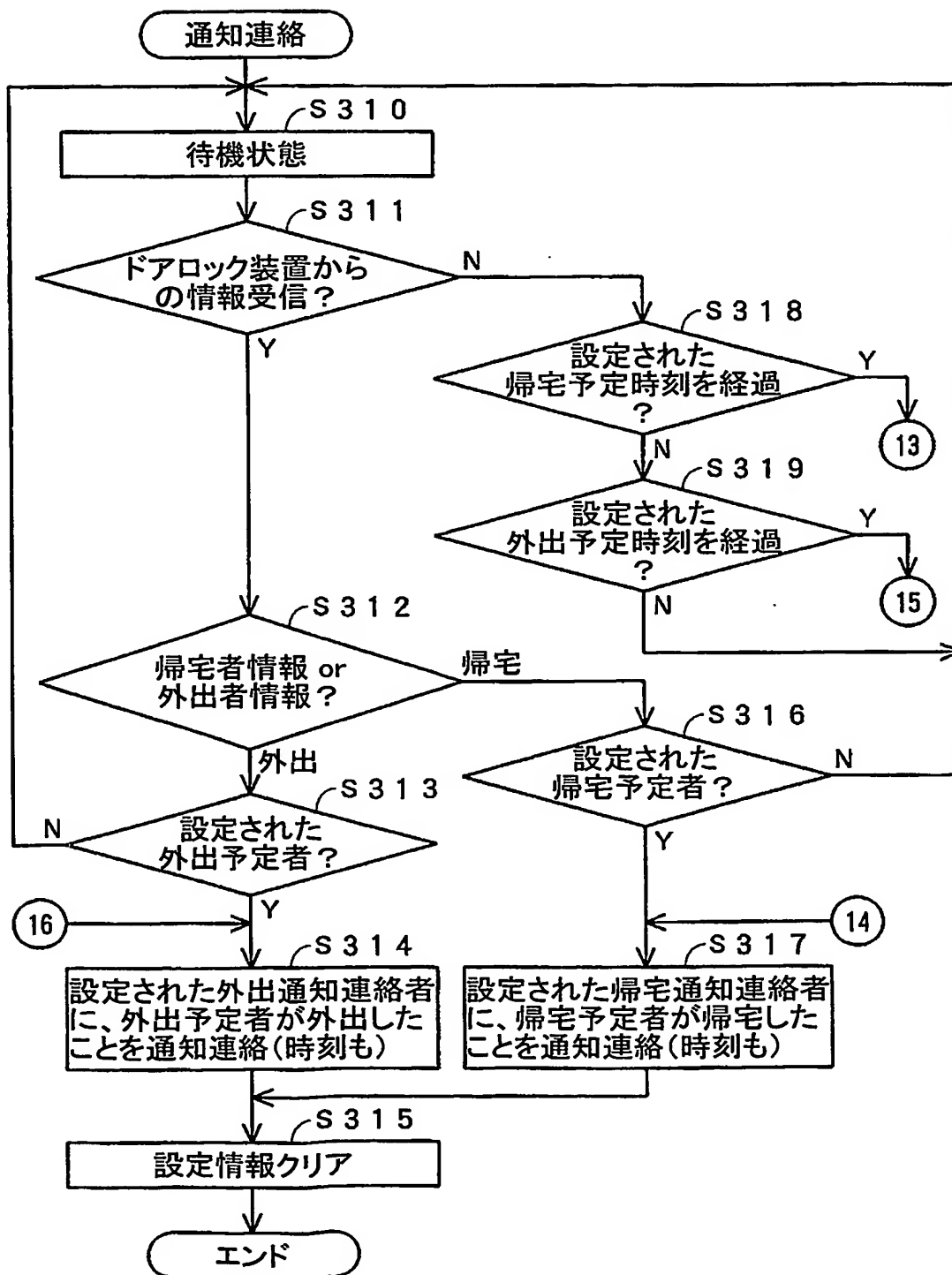


Fig.38

37/38

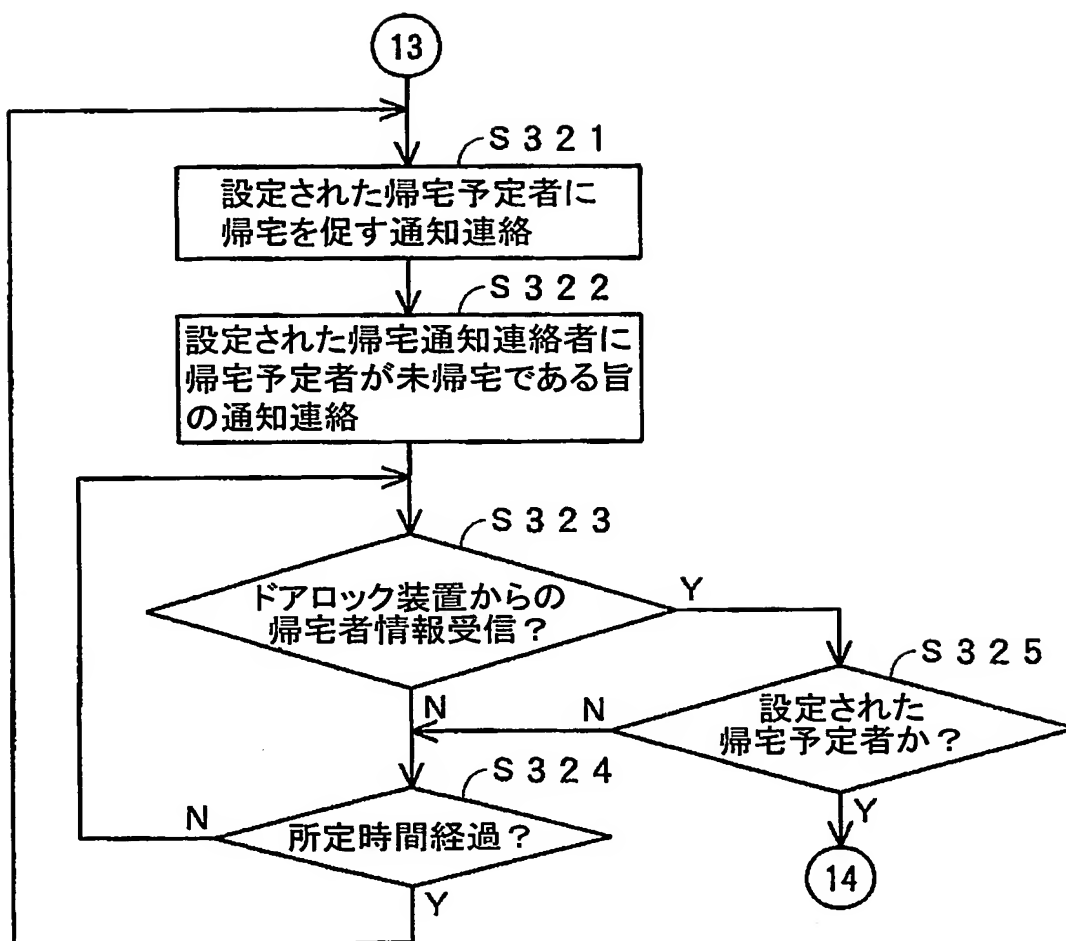


Fig.39

38/38

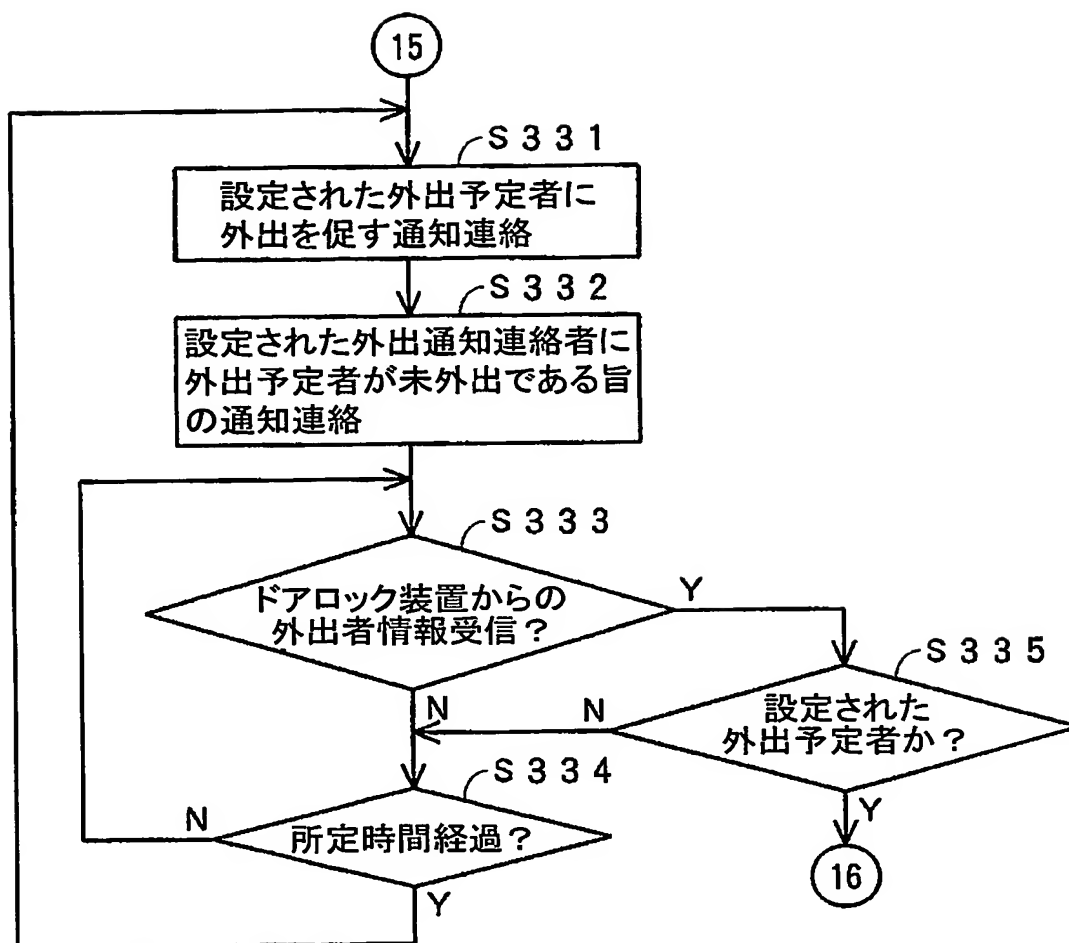


Fig.40

INTERNATIONAL SEARCH REPORT

International Application No.
PCT/JP03/09755

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ E05B49/00, G08B25/04

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ E05B49/00-49/04, G08B23/00-31/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Toroku Jitsuyo Shinan Koho	1994-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2002-70377 A (Yokogawa Electric Corp.), 08 March, 2002 (08.03.02), Full text; all drawings (Family: none)	1, 7 2-6, 8
Y	JP 2002-16714 A (Matsushita Electric Works, Ltd.), 18 January, 2002 (18.01.02), Full text; all drawings (Family: none)	2-6, 8
Y	JP 2000-259971 A (Kabushiki Kaisha Shin Shakai Shihon Joho Kaihatsu Center), 22 September, 2000 (22.09.00), Full text; all drawings (Family: none)	3-6

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

<p>* Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p>	<p>"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art</p> <p>"&" document member of the same patent family</p>
--	---

Date of the actual completion of the international search 05 September, 2003 (05.09.03)	Date of mailing of the international search report 07 October, 2003 (07.10.03)
--	---

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International Application No.

PCT/JP03/09755

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2000-268273 A (Aichi Tokei Denki Kabushiki Kaisha), 29 September, 2000 (29.09.00), Par. No. [0004] (Family: none)	3
Y	JP 11-45392 A (Matsushita Electric Works, Ltd.), 16 February, 1999 (16.02.99), Par. No. [0012] (Family: none)	3
Y	JP 2002-71478 A (Hitachi Government & Public Corporation System Engineering, Ltd.), 08 March, 2002 (08.03.02), Par. Nos. [0008] to [0010]; Fig. 1 (Family: none)	4

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ E05B49/00, G08B25/04

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ E05B49/00-49/04, G08B23/00-31/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2003年
日本国実用新案登録公報	1996-2003年
日本国登録実用新案公報	1994-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	JP 2002-70377 A (横河電機株式会社) 2002.03.08, 全文, 全図 (ファミリーなし)	1, 7
Y		2-6, 8
Y	JP 2002-16714 A (松下電工株式会社) 2002.01.18, 全文, 全図 (ファミリーなし)	2-6, 8

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

05.09.03

国際調査報告の発送日

07.10.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

清藤 弘晃



2R

2916

電話番号 03-3581-1101 内線 3422

C (続き). 関連すると認められる文献